

## MCAFFEE FOUNDSTONE FSL UPDATE

To better protect your environment McAfee has created this FSL check update for the Foundstone Product Suite. The following is a detailed summary of the new and updated checks included with this release.

### NEW CHECKS

#### 21529 - Google Chrome Multiple Vulnerabilities Prior To 57.0.2987.98

Category: Windows Host Assessment -> Miscellaneous  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2017-5029, CVE-2017-5030, CVE-2017-5031, CVE-2017-5032, CVE-2017-5033, CVE-2017-5034, CVE-2017-5035, CVE-2017-5036, CVE-2017-5037, CVE-2017-5038, CVE-2017-5039, CVE-2017-5040, CVE-2017-5041, CVE-2017-5042, CVE-2017-5043, CVE-2017-5044, CVE-2017-5045, CVE-2017-5046

#### Description

Multiple vulnerabilities are present in some versions of Google Chrome.

#### Observation

Google Chrome is a popular web browser.

Multiple vulnerabilities are present in some versions of Google Chrome. The flaws lie in multiple components. Successful exploitation could allow an attacker to bypass certain security restrictions, retrieve sensitive data, conduct spoofing attacks, cause a denial of service, or execute arbitrary code.

#### 21530 - Google Chrome Multiple Vulnerabilities Prior To 57.0.2987.98

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2017-5029, CVE-2017-5030, CVE-2017-5031, CVE-2017-5032, CVE-2017-5033, CVE-2017-5034, CVE-2017-5035, CVE-2017-5036, CVE-2017-5037, CVE-2017-5038, CVE-2017-5039, CVE-2017-5040, CVE-2017-5041, CVE-2017-5042, CVE-2017-5043, CVE-2017-5044, CVE-2017-5045, CVE-2017-5046

#### Description

Multiple vulnerabilities are present in some versions of Google Chrome.

#### Observation

Google Chrome is a popular web browser.

Multiple vulnerabilities are present in some versions of Google Chrome. The flaws lie in multiple components. Successful exploitation could allow an attacker to bypass certain security restrictions, retrieve sensitive data, conduct spoofing attacks, cause a denial of service, or execute arbitrary code.

#### 163304 - Oracle Enterprise Linux ELSA-2017-0662 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Oracle Enterprise Linux Patches and Hotfixes

Risk Level: High

CVE: CVE-2007-2444, CVE-2007-2446, CVE-2007-2447, CVE-2008-1105, CVE-2008-3789, CVE-2008-4314, CVE-2009-2813, CVE-2009-2906, CVE-2009-2948, CVE-2009-3297, CVE-2010-0728, CVE-2010-3069, CVE-2011-0719, CVE-2011-2522, CVE-2011-2694,

CVE-2012-1182, CVE-2012-2111, CVE-2012-6150, CVE-2013-0213, CVE-2013-0214, CVE-2013-4124, CVE-2013-4408, CVE-2013-4475, CVE-2013-4496, CVE-2013-6442, CVE-2014-0244, CVE-2014-3493, CVE-2015-0240, CVE-2015-5252, CVE-2015-5296, CVE-2015-5299, CVE-2015-5330, CVE-2015-5370, CVE-2015-7560, CVE-2016-2110, CVE-2016-2111, CVE-2016-2112, CVE-2016-2115, CVE-2016-2118, CVE-2016-2125, CVE-2016-2126

#### Description

The scan detected that the host is missing the following update:  
ELSA-2017-0662

#### Observation

Updates often remediate critical security problems that should be quickly addressed.  
For more information see:

<http://oss.oracle.com/pipermail/el-errata/2017-March/006812.html>

#### OEL6

##### x86\_64

libsmbclient-devel-3.6.23-41.0.1.el6  
samba-winbind-devel-3.6.23-41.0.1.el6  
samba-swat-3.6.23-41.0.1.el6  
samba-glusterfs-3.6.23-41.0.1.el6  
samba-client-3.6.23-41.0.1.el6  
samba-3.6.23-41.0.1.el6  
samba-winbind-3.6.23-41.0.1.el6  
samba-domainjoin-gui-3.6.23-41.0.1.el6  
samba-winbind-clients-3.6.23-41.0.1.el6  
samba-doc-3.6.23-41.0.1.el6  
samba-common-3.6.23-41.0.1.el6  
libsmbclient-3.6.23-41.0.1.el6  
samba-winbind-krb5-locator-3.6.23-41.0.1.el6

##### i386

samba-3.6.23-41.0.1.el6  
samba-common-3.6.23-41.0.1.el6  
samba-winbind-clients-3.6.23-41.0.1.el6  
samba-winbind-3.6.23-41.0.1.el6  
samba-domainjoin-gui-3.6.23-41.0.1.el6  
samba-client-3.6.23-41.0.1.el6  
samba-winbind-krb5-locator-3.6.23-41.0.1.el6  
libsmbclient-3.6.23-41.0.1.el6  
samba-doc-3.6.23-41.0.1.el6  
samba-winbind-devel-3.6.23-41.0.1.el6  
libsmbclient-devel-3.6.23-41.0.1.el6  
samba-swat-3.6.23-41.0.1.el6

### 163310 - Oracle Enterprise Linux ELSA-2017-0817 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Oracle Enterprise Linux Patches and Hotfixes

Risk Level: High

CVE: CVE-2016-10088, CVE-2016-10142, CVE-2016-1583, CVE-2016-2069, CVE-2016-2143, CVE-2016-2384, CVE-2016-4470, CVE-2016-4565, CVE-2016-4998, CVE-2016-5195, CVE-2016-5696, CVE-2016-5829, CVE-2016-6136, CVE-2016-6480, CVE-2016-6828, CVE-2016-7042, CVE-2016-7097, CVE-2016-7117, CVE-2016-8399, CVE-2016-9555, CVE-2016-9576, CVE-2017-6074

#### Description

The scan detected that the host is missing the following update:  
ELSA-2017-0817

## Observation

Updates often remediate critical security problems that should be quickly addressed.  
For more information see:

<http://oss.oracle.com/pipermail/el-errata/2017-March/006808.html>

## OEL6

x86\_64  
python-perf-2.6.32-696.el6  
kernel-2.6.32-696.el6  
kernel-firmware-2.6.32-696.el6  
kernel-doc-2.6.32-696.el6  
perf-2.6.32-696.el6  
kernel-debug-2.6.32-696.el6  
kernel-abi-whitelists-2.6.32-696.el6  
kernel-headers-2.6.32-696.el6  
kernel-debug-devel-2.6.32-696.el6  
kernel-devel-2.6.32-696.el6

## i386

python-perf-2.6.32-696.el6  
kernel-2.6.32-696.el6  
kernel-firmware-2.6.32-696.el6  
kernel-doc-2.6.32-696.el6  
perf-2.6.32-696.el6  
kernel-debug-2.6.32-696.el6  
kernel-abi-whitelists-2.6.32-696.el6  
kernel-headers-2.6.32-696.el6  
kernel-debug-devel-2.6.32-696.el6  
kernel-devel-2.6.32-696.el6

## **21546 - (VMSA-2017-0004) VMware vCenter Server Apache Struts 2 RCE Vulnerability**

Category: Windows Host Assessment -> Miscellaneous  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2017-5638

## Description

A vulnerability is present in some versions of VMware vCenter Server.

## Observation

VMware vCenter Server is a scalable and extensible platform to manage VMware vSphere.

A vulnerability is present in some versions of VMware vCenter Server. The flaw lies in Apache Struts 2 component. Successful exploitation could allow an attacker to execute remote code.

## **21547 - (VMSA-2017-0004) VMware vCenter Server Apache Struts 2 RCE Vulnerability**

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2017-5638

## Description

A vulnerability is present in some versions of VMware vCenter Server.

## Observation

VMware vCenter Server is a scalable and extensible platform to manage VMware vSphere.

A vulnerability is present in some versions of VMware vCenter Server. The flaw lies in Apache Struts 2 component. Successful exploitation could allow an attacker to execute remote code.

## **163314 - Oracle Enterprise Linux ELSA-2017-0621 Update Is Not Installed**

Category: SSH Module -> NonIntrusive -> Oracle Enterprise Linux Patches and Hotfixes

Risk Level: High

CVE: CVE-2010-0431, CVE-2010-2784, CVE-2011-0011, CVE-2011-1750, CVE-2011-1751, CVE-2011-2212, CVE-2011-2527, CVE-2011-4111, CVE-2011-4127, CVE-2012-0029, CVE-2012-2652, CVE-2012-3515, CVE-2012-6075, CVE-2013-2007, CVE-2013-2231, CVE-2013-4148, CVE-2013-4151, CVE-2013-4344, CVE-2013-4535, CVE-2013-4536, CVE-2013-4541, CVE-2013-4542, CVE-2013-6399, CVE-2014-0142, CVE-2014-0143, CVE-2014-0144, CVE-2014-0145, CVE-2014-0146, CVE-2014-0147, CVE-2014-0150, CVE-2014-0182, CVE-2014-0222, CVE-2014-0223, CVE-2014-2894, CVE-2014-3461, CVE-2014-3640, CVE-2014-7815, CVE-2014-7840, CVE-2014-8106, CVE-2015-3209, CVE-2015-3456, CVE-2015-5165, CVE-2015-5279, CVE-2015-7512, CVE-2016-1714, CVE-2016-2857, CVE-2016-3710, CVE-2016-3712, CVE-2016-5403, CVE-2017-2615, CVE-2017-2620

## Description

The scan detected that the host is missing the following update:  
ELSA-2017-0621

## Observation

Updates often remediate critical security problems that should be quickly addressed.  
For more information see:

<http://oss.oracle.com/pipermail/el-errata/2017-March/006805.html>

## OEL6

x86\_64

qemu-kvm-tools-0.12.1.2-2.503.el6

qemu-guest-agent-0.12.1.2-2.503.el6

qemu-img-0.12.1.2-2.503.el6

qemu-kvm-0.12.1.2-2.503.el6

## i386

qemu-guest-agent-0.12.1.2-2.503.el6

## **21514 - D-link Dir-850l Web Admin Interface Stack-based Buffer Overflow Vulnerability**

Category: Wireless Assessment -> NonIntrusive -> Wireless

Risk Level: High

CVE: CVE-2017-3193

## Description

A buffer overflow vulnerability is present in some versions of D-Link DIR-model.

## Observation

D-Link DIR is a wireless router.

A buffer overflow vulnerability is present in some versions of D-Link DIR-model. The flaw lies in the web administration interface HNAP service. Successful exploitation could allow an attacker to remotely execute arbitrary code.

## **21540 - (CTX221578) Citrix XenServer Vulnerability**

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2016-9603

#### Description

A buffer overflow vulnerability is present in some versions of Citrix XenServer.

#### Observation

Citrix XenServer is a popular virtualization platform.

A buffer overflow vulnerability is present in some versions of Citrix XenServer. The flaw lies in Quick emulator (QEMU). Successful exploitation could allow the administrator of an HVM guest VM to compromise the host.

### **21329 - (K50459349) F5 BIG-IP Expat XML Library Vulnerability**

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2015-2716

#### Description

A remote code execution vulnerability is present in some versions of F5's BIG-IP Products.

#### Observation

F5's BIG-IP Products are network appliances that run F5's Traffic Management Operating System.

A remote code execution vulnerability is present in some versions of F5's BIG-IP Products. The flaw lies in the XML parser used by Mozilla Firefox and Mozilla Thunderbird. Successful exploitation could allow an attacker to remotely execute arbitrary code.

### **21508 - Mozilla Firefox Multiple Vulnerabilities Prior To 52**

Category: Windows Host Assessment -> Miscellaneous  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2017-5398, CVE-2017-5399, CVE-2017-5400, CVE-2017-5401, CVE-2017-5402, CVE-2017-5403, CVE-2017-5404, CVE-2017-5405, CVE-2017-5406, CVE-2017-5407, CVE-2017-5408, CVE-2017-5409, CVE-2017-5410, CVE-2017-5411, CVE-2017-5412, CVE-2017-5413, CVE-2017-5414, CVE-2017-5415, CVE-2017-5416, CVE-2017-5417, CVE-2017-5418, CVE-2017-5419, CVE-2017-5420, CVE-2017-5421, CVE-2017-5422, CVE-2017-5425, CVE-2017-5426, CVE-2017-5427

#### Description

Multiple vulnerabilities are present in some versions of Mozilla Firefox.

#### Observation

Mozilla Firefox is a popular web browser.

Multiple vulnerabilities are present in some versions of Mozilla Firefox. The flaws lie in several components. Successful exploitation could allow an attacker to obtain sensitive information or cause a denial of service condition or execute arbitrary code.

### **21509 - Mozilla Firefox Multiple Vulnerabilities Prior To 52**

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2017-5398, CVE-2017-5399, CVE-2017-5400, CVE-2017-5401, CVE-2017-5402, CVE-2017-5403, CVE-2017-5404, CVE-2017-5405, CVE-2017-5406, CVE-2017-5407, CVE-2017-5408, CVE-2017-5409, CVE-2017-5410, CVE-2017-5411, CVE-2017-5412,

CVE-2017-5413, CVE-2017-5414, CVE-2017-5415, CVE-2017-5416, CVE-2017-5417, CVE-2017-5418, CVE-2017-5419, CVE-2017-5420, CVE-2017-5421, CVE-2017-5422, CVE-2017-5425, CVE-2017-5426, CVE-2017-5427

#### Description

Multiple vulnerabilities are present in some versions of Mozilla Firefox.

#### Observation

Mozilla Firefox is a popular web browser.

Multiple vulnerabilities are present in some versions of Mozilla Firefox. The flaws lie in several components. Successful exploitation could allow an attacker to obtain sensitive information or cause a denial of service condition or execute arbitrary code.

### **21519 - (K49144112) F5 BIG-IP Tcpcdump Multiple Vulnerabilities**

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2016-7934, CVE-2016-7935, CVE-2016-7936, CVE-2016-7937, CVE-2016-7939

#### Description

Multiple vulnerabilities are present in some versions of F5's BIG-IP products.

#### Observation

F5's BIG-IP products are network appliances that run F5's Traffic Management Operating System.

Multiple vulnerabilities are present in some versions of F5's BIG-IP products. The flaws lie in the tcpcdump component. Successful exploitation could allow an attacker to retrieve sensitive data or to cause a denial of service condition.

### **21520 - (K31997425) F5 BIG-IP Tcpcdump Multiple Vulnerabilities**

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2017-5482, CVE-2017-5483, CVE-2017-5484, CVE-2017-5485, CVE-2017-5486

#### Description

Multiple vulnerabilities are present in some versions of F5's BIG-IP products.

#### Observation

F5's BIG-IP products are network appliances that run F5's Traffic Management Operating System.

Multiple vulnerabilities are present in some versions of F5's BIG-IP products. The flaws lie in the tcpcdump component. Successful exploitation could allow an attacker to retrieve sensitive data or to cause a denial of service condition.

### **21521 - (K39512927) F5 BIG-IP Tcpcdump Multiple Vulnerabilities**

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2016-7928, CVE-2016-7929, CVE-2016-7930, CVE-2016-7931, CVE-2016-7933

#### Description

Multiple vulnerabilities are present in some versions of F5's BIG-IP products.

#### Observation

F5's BIG-IP products are network appliances that run F5's Traffic Management Operating System.

Multiple vulnerabilities are present in some versions of F5's BIG-IP products. The flaws lie in the tcpdump component. Successful exploitation could allow an attacker to retrieve sensitive data or to cause a denial of service condition.

#### **21522 - (K94010578) F5 BIG-IP Tcpdump Multiple Vulnerabilities**

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2016-7940, CVE-2016-7973, CVE-2016-7974, CVE-2016-7983, CVE-2016-7984

##### Description

Multiple vulnerabilities are present in some versions of F5's BIG-IP products.

##### Observation

F5's BIG-IP products are network appliances that run F5's Traffic Management Operating System.

Multiple vulnerabilities are present in some versions of F5's BIG-IP products. The flaws lie in the tcpdump component. Successful exploitation could allow an attacker to retrieve sensitive data or to cause a denial of service condition.

#### **21523 - (K77384526) F5 BIG-IP Tcpdump Multiple Vulnerabilities**

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2016-7922, CVE-2016-7923, CVE-2016-7924, CVE-2016-7925, CVE-2016-7927

##### Description

Multiple vulnerabilities are present in some versions of F5's BIG-IP products.

##### Observation

F5's BIG-IP products are network appliances that run F5's Traffic Management Operating System.

Multiple vulnerabilities are present in some versions of F5's BIG-IP products. The flaws lie in the tcpdump component. Successful exploitation could allow an attacker to retrieve sensitive data or to cause a denial of service condition.

#### **21524 - (K72403108) F5 BIG-IP Tcpdump Multiple Vulnerabilities**

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2016-7926, CVE-2016-7932, CVE-2016-7938

##### Description

Multiple vulnerabilities are present in some versions of F5's BIG-IP products.

##### Observation

F5's BIG-IP products are network appliances that run F5's Traffic Management Operating System.

Multiple vulnerabilities are present in some versions of F5's BIG-IP products. The flaws lie in the tcpdump component. Successful exploitation could allow an attacker to retrieve sensitive data or to cause a denial of service condition.

#### **21525 - (K94778122) F5 BIG-IP Tcpdump Multiple Vulnerabilities**

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2016-7985, CVE-2016-7992, CVE-2016-7993, CVE-2016-8574, CVE-2016-8575

#### Description

Multiple vulnerabilities are present in some versions of F5's BIG-IP products.

#### Observation

F5's BIG-IP products are network appliances that run F5's Traffic Management Operating System.

Multiple vulnerabilities are present in some versions of F5's BIG-IP products. The flaws lie in the tcpdump component. Successful exploitation could allow an attacker to retrieve sensitive data or to cause a denial of service condition.

### **21526 - (K55129614) F5 BIG-IP Tcpdump Multiple Vulnerabilities**

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2016-5341, CVE-2016-7975, CVE-2016-7986

#### Description

Multiple vulnerabilities are present in some versions of F5's BIG-IP products.

#### Observation

F5's BIG-IP products are network appliances that run F5's Traffic Management Operating System.

Multiple vulnerabilities are present in some versions of F5's BIG-IP products. The flaws lie in the tcpdump component. Successful exploitation could allow an attacker to retrieve sensitive data or to cause a denial of service condition.

### **21527 - (K04225025) F5 BIG-IP Tcpdump Multiple Vulnerabilities**

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2017-5202, CVE-2017-5203, CVE-2017-5204, CVE-2017-5205, CVE-2017-5342

#### Description

Multiple vulnerabilities are present in some versions of F5's BIG-IP products.

#### Observation

F5's BIG-IP products are network appliances that run F5's Traffic Management Operating System.

Multiple vulnerabilities are present in some versions of F5's BIG-IP products. The flaws lie in the tcpdump component. Successful exploitation could allow an attacker to retrieve sensitive data or to cause a denial of service condition.

### **21543 - (VMSA-2017-0005) VMware Workstation Player Out Of Bounds Memory Access Vulnerability**

Category: Windows Host Assessment -> Miscellaneous  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2017-4901

#### Description

An out-of-bounds memory access vulnerability is present in some versions of VMware Workstation Player.



### Observation

VMware Workstation Player is used to run VMware virtual machine.

An out-of-bounds memory access vulnerability is present in some versions of VMware Workstation Player. The flaw lies in drag-and-drop (DnD) function. Successful exploit could allow an attacker to execute code on host operating system.

## **21545 - IBM WebSphere Application Server Privilege Escalation Vulnerability (swg21999293)**

Category: Windows Host Assessment -> Miscellaneous  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2017-1151

### Description

A privilege escalation vulnerability is present in some versions of IBM WebSphere Application Server.

### Observation

IBM WebSphere Application Server is a Java application server.

A privilege escalation vulnerability is present in some versions of IBM WebSphere Application Server. The flaw lies in the OpenID Connect (OIDC), Trust Association Interceptor (TAI) component. Successful exploitation could allow an attacker to obtain elevated privileges on the system.

## **21548 - (VMSA-2017-0005) VMware Workstation Pro Out Of Bounds Memory Access Vulnerability**

Category: Windows Host Assessment -> Miscellaneous  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2017-4901

### Description

A vulnerability is present in some versions of VMware Workstation.

### Observation

VMware Workstation is a virtualization software.

A vulnerability is present in some versions of VMware Workstation. The flaw lies in drag-and-drop (DnD) function. Successful exploit could allow an attacker to execute code on host operating system.

## **132344 - Oracle VM OVMSA-2017-0048 Update Is Not Installed**

Category: SSH Module -> NonIntrusive -> Oracle VM Patches and Hotfixes

Risk Level: High

CVE: CVE-2013-1447, CVE-2013-6045, CVE-2013-6052, CVE-2013-6054, CVE-2016-5139, CVE-2016-5158, CVE-2016-5159, CVE-2016-7163, CVE-2016-9675

### Description

The scan detected that the host is missing the following update:  
OVMSA-2017-0048

### Observation

Updates often remediate critical security problems that should be quickly addressed.  
For more information see:

<http://oss.oracle.com/pipermail/oraclevm-errata/2017-March/000658.html>  
<http://oss.oracle.com/pipermail/oraclevm-errata/2017-March/000657.html>

OVM3.3  
x86\_64  
openjpeg-libs-1.3-16.el6\_8

OVM3.4  
x86\_64  
openjpeg-libs-1.3-16.el6\_8

## 141526 - Red Hat Enterprise Linux RHSA-2017-0838 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Red Hat Enterprise Linux Patches and Hotfixes

Risk Level: High

CVE: CVE-2013-6045, CVE-2016-5139, CVE-2016-5158, CVE-2016-5159, CVE-2016-7163, CVE-2016-9573, CVE-2016-9675

### Description

The scan detected that the host is missing the following update:  
RHSA-2017-0838

### Observation

Updates often remediate critical security problems that should be quickly addressed.  
For more information see:

<https://rhn.redhat.com/errata/RHSA-2017-0838.html>

RHEL7D  
x86\_64  
openjpeg-1.5.1-16.el7\_3  
openjpeg-libs-1.5.1-16.el7\_3  
openjpeg-debuginfo-1.5.1-16.el7\_3  
openjpeg-devel-1.5.1-16.el7\_3

RHEL7S  
x86\_64  
openjpeg-1.5.1-16.el7\_3  
openjpeg-libs-1.5.1-16.el7\_3  
openjpeg-debuginfo-1.5.1-16.el7\_3  
openjpeg-devel-1.5.1-16.el7\_3

RHEL7WS  
x86\_64  
openjpeg-1.5.1-16.el7\_3  
openjpeg-libs-1.5.1-16.el7\_3  
openjpeg-debuginfo-1.5.1-16.el7\_3  
openjpeg-devel-1.5.1-16.el7\_3

## 145272 - SuSE SLES 12 SP2 SUSE-SU-2017:0797-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: High

CVE: CVE-2016-0736, CVE-2016-2161, CVE-2016-8743

### Description

The scan detected that the host is missing the following update:

SUSE-SU-2017:0797-1

### Observation

Updates often remediate critical security problems that should be quickly addressed.  
For more information see:

<http://lists.suse.com/pipermail/sle-security-updates/2017-March/002737.html>

SuSE SLES 12 SP2

noarch  
apache2-doc-2.4.23-21.1

x86\_64  
apache2-2.4.23-21.1  
apache2-debuginfo-2.4.23-21.1  
apache2-utils-debuginfo-2.4.23-21.1  
apache2-worker-debuginfo-2.4.23-21.1  
apache2-debugsource-2.4.23-21.1  
apache2-utils-2.4.23-21.1  
apache2-example-pages-2.4.23-21.1  
apache2-prefork-2.4.23-21.1  
apache2-prefork-debuginfo-2.4.23-21.1  
apache2-worker-2.4.23-21.1

## 145274 - SuSE SLES 11 SP4 SUSE-SU-2017:0841-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: High

CVE: CVE-2017-2619

### Description

The scan detected that the host is missing the following update:  
SUSE-SU-2017:0841-1

### Observation

Updates often remediate critical security problems that should be quickly addressed.  
For more information see:

<http://lists.suse.com/pipermail/sle-security-updates/2017-March/002743.html>

SuSE SLES 11 SP4

noarch  
samba-doc-3.6.3-87.1

i586  
samba-3.6.3-87.1  
samba-winbind-3.6.3-87.1  
libtdb1-3.6.3-87.1  
libwbclient0-3.6.3-87.1  
libtevent0-3.6.3-87.1  
samba-krb-printing-3.6.3-87.1  
libsmbclient0-3.6.3-87.1  
samba-client-3.6.3-87.1  
libtalloc2-3.6.3-87.1  
ldapsmb-1.34b-87.1  
libldb1-3.6.3-87.1

x86\_64  
samba-client-32bit-3.6.3-87.1  
libwbclient0-3.6.3-87.1  
samba-3.6.3-87.1  
libtdb1-32bit-3.6.3-87.1  
libsmbclient0-32bit-3.6.3-87.1  
samba-krb-printing-3.6.3-87.1  
libtevent0-32bit-3.6.3-87.1  
libtevent0-3.6.3-87.1  
libldb1-3.6.3-87.1  
libtalloc2-3.6.3-87.1  
libtdb1-3.6.3-87.1  
samba-client-3.6.3-87.1  
libsmbclient0-3.6.3-87.1  
ldapsmb-1.34b-87.1  
libwbclient0-32bit-3.6.3-87.1  
samba-32bit-3.6.3-87.1  
samba-winbind-32bit-3.6.3-87.1  
libtalloc2-32bit-3.6.3-87.1  
samba-winbind-3.6.3-87.1

### 145277 - SuSE SLES 12 SP1 SUSE-SU-2017:0801-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: High

CVE: CVE-2016-0736, CVE-2016-2161, CVE-2016-8743

#### Description

The scan detected that the host is missing the following update:  
SUSE-SU-2017:0801-1

#### Observation

Updates often remediate critical security problems that should be quickly addressed.  
For more information see:

<http://lists.suse.com/pipermail/sle-security-updates/2017-March/002741.html>

SuSE SLES 12 SP1

noarch  
apache2-doc-2.4.16-19.1

x86\_64  
apache2-utils-debuginfo-2.4.16-19.1  
apache2-prefork-2.4.16-19.1  
apache2-utils-2.4.16-19.1  
apache2-prefork-debuginfo-2.4.16-19.1  
apache2-worker-debuginfo-2.4.16-19.1  
apache2-worker-2.4.16-19.1  
apache2-example-pages-2.4.16-19.1  
apache2-debuginfo-2.4.16-19.1  
apache2-debugsource-2.4.16-19.1  
apache2-2.4.16-19.1

### 163307 - Oracle Enterprise Linux ELSA-2017-0680 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Oracle Enterprise Linux Patches and Hotfixes

Risk Level: High

CVE: CVE-2014-9761, CVE-2015-8776, CVE-2015-8778, CVE-2015-8779

### Description

The scan detected that the host is missing the following update:  
ELSA-2017-0680

### Observation

Updates often remediate critical security problems that should be quickly addressed.  
For more information see:

<http://oss.oracle.com/pipermail/el-errata/2017-March/006803.html>

#### OEL6

x86\_64  
glibc-2.12-1.209.0.1.el6  
glibc-static-2.12-1.209.0.1.el6  
glibc-headers-2.12-1.209.0.1.el6  
glibc-devel-2.12-1.209.0.1.el6  
glibc-utils-2.12-1.209.0.1.el6  
glibc-common-2.12-1.209.0.1.el6  
nscd-2.12-1.209.0.1.el6

#### i386

glibc-2.12-1.209.0.1.el6  
glibc-static-2.12-1.209.0.1.el6  
glibc-headers-2.12-1.209.0.1.el6  
glibc-devel-2.12-1.209.0.1.el6  
glibc-utils-2.12-1.209.0.1.el6  
glibc-common-2.12-1.209.0.1.el6  
nscd-2.12-1.209.0.1.el6

## 163309 - Oracle Enterprise Linux ELSA-2017-0794 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Oracle Enterprise Linux Patches and Hotfixes

Risk Level: High

CVE: CVE-2011-3323, CVE-2011-3324, CVE-2011-3325, CVE-2011-3326, CVE-2011-3327, CVE-2012-0249, CVE-2012-0250, CVE-2012-0255, CVE-2012-1820, CVE-2013-2236, CVE-2016-1245, CVE-2016-2342, CVE-2016-4049, CVE-2017-5495

### Description

The scan detected that the host is missing the following update:  
ELSA-2017-0794

### Observation

Updates often remediate critical security problems that should be quickly addressed.  
For more information see:

<http://oss.oracle.com/pipermail/el-errata/2017-March/006802.html>

#### OEL6

x86\_64  
quagga-contrib-0.99.15-14.el6  
quagga-devel-0.99.15-14.el6  
quagga-0.99.15-14.el6

#### i386

quagga-contrib-0.99.15-14.el6  
quagga-devel-0.99.15-14.el6

## 163312 - Oracle Enterprise Linux ELSA-2017-0574 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Oracle Enterprise Linux Patches and Hotfixes

Risk Level: High

CVE: CVE-2016-8610, CVE-2017-5335, CVE-2017-5336, CVE-2017-5337

### Description

The scan detected that the host is missing the following update:  
ELSA-2017-0574

### Observation

Updates often remediate critical security problems that should be quickly addressed.  
For more information see:

<http://oss.oracle.com/pipermail/el-errata/2017-March/006797.html>

#### OEL6

x86\_64

gnutls-devel-2.12.23-21.el6

gnutls-2.12.23-21.el6

gnutls-guile-2.12.23-21.el6

gnutls-utils-2.12.23-21.el6

#### i386

gnutls-devel-2.12.23-21.el6

gnutls-2.12.23-21.el6

gnutls-guile-2.12.23-21.el6

gnutls-utils-2.12.23-21.el6

## 163313 - Oracle Enterprise Linux ELSA-2017-0641 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Oracle Enterprise Linux Patches and Hotfixes

Risk Level: High

CVE: CVE-2015-8325

### Description

The scan detected that the host is missing the following update:  
ELSA-2017-0641

### Observation

Updates often remediate critical security problems that should be quickly addressed.  
For more information see:

<http://oss.oracle.com/pipermail/el-errata/2017-March/006798.html>

#### OEL6

x86\_64

openssh-5.3p1-122.el6

openssh-clients-5.3p1-122.el6

openssh-server-5.3p1-122.el6

openssh-lldap-5.3p1-122.el6

pam\_ssh\_agent\_auth-0.9.3-122.el6

openssh-askpass-5.3p1-122.el6

i386  
openssh-5.3p1-122.el6  
openssh-clients-5.3p1-122.el6  
openssh-server-5.3p1-122.el6  
openssh-ldap-5.3p1-122.el6  
pam\_ssh\_agent\_auth-0.9.3-122.el6  
openssh-askpass-5.3p1-122.el6

### 163315 - Oracle Enterprise Linux ELSA-2017-0631 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Oracle Enterprise Linux Patches and Hotfixes

Risk Level: High

CVE: CVE-2013-4075, CVE-2015-3811, CVE-2015-3812, CVE-2015-3813

#### Description

The scan detected that the host is missing the following update:  
ELSA-2017-0631

#### Observation

Updates often remediate critical security problems that should be quickly addressed.  
For more information see:

<http://oss.oracle.com/pipermail/el-errata/2017-March/006810.html>

OEL6  
x86\_64  
wireshark-gnome-1.8.10-25.0.1.el6  
wireshark-1.8.10-25.0.1.el6  
wireshark-devel-1.8.10-25.0.1.el6

i386  
wireshark-gnome-1.8.10-25.0.1.el6  
wireshark-1.8.10-25.0.1.el6  
wireshark-devel-1.8.10-25.0.1.el6

### 163317 - Oracle Enterprise Linux ELSA-2017-0725 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Oracle Enterprise Linux Patches and Hotfixes

Risk Level: High

CVE: CVE-2016-0634, CVE-2016-7543, CVE-2016-9401

#### Description

The scan detected that the host is missing the following update:  
ELSA-2017-0725

#### Observation

Updates often remediate critical security problems that should be quickly addressed.  
For more information see:

<http://oss.oracle.com/pipermail/el-errata/2017-March/006800.html>

OEL6  
x86\_64  
bash-4.1.2-48.el6  
bash-doc-4.1.2-48.el6

i386  
bash-4.1.2-48.el6  
bash-doc-4.1.2-48.el6

### 185642 - Ubuntu Linux 12.04 USN-3239-3 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Ubuntu Patches and Hotfixes

Risk Level: High

CVE: CVE-2015-8982, CVE-2015-8983, CVE-2015-8984, CVE-2016-1234, CVE-2016-3706, CVE-2016-4429, CVE-2016-5417, CVE-2016-6323

#### Description

The scan detected that the host is missing the following update:  
USN-3239-3

#### Observation

Updates often remediate critical security problems that should be quickly addressed.  
For more information see:

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2017-March/003791.html>

Ubuntu 12.04

libc6\_2.15-0ubuntu10.18

### 191870 - Fedora Linux 24 FEDORA-2017-3b97b275da Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: High

CVE: CVE-2016-6525, CVE-2016-8674, CVE-2017-5896, CVE-2017-6060

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2017-3b97b275da

#### Observation

Updates often remediate critical security problems that should be quickly addressed.  
For more information see:

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/3/?count=200&page=4>

Fedora Core 24

mupdf-1.10a-4.fc24

### 191879 - Fedora Linux 25 FEDORA-2017-47a4910f07 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: High

CVE: CVE-2016-7567

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2017-47a4910f07



### Observation

Updates often remediate critical security problems that should be quickly addressed.

For more information see:

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/3/?count=200&page=4>

Fedora Core 25

openslp-2.0.0-10.fc25

### **130728 - Debian Linux 8.0 DSA-3814-1 Update Is Not Installed**

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2017-6827, CVE-2017-6828, CVE-2017-6829, CVE-2017-6830, CVE-2017-6831, CVE-2017-6832, CVE-2017-6833, CVE-2017-6834, CVE-2017-6835, CVE-2017-6836, CVE-2017-6837, CVE-2017-6838, CVE-2017-6839

### Description

The scan detected that the host is missing the following update:

DSA-3814-1

### Observation

Updates often remediate critical security problems that should be quickly addressed.

For more information see:

<http://www.debian.org/security/2017/dsa-3814>

Debian 8.0

all

audiofile-tools\_0.3.6-2+deb8u2

libaudiofile-dev\_0.3.6-2+deb8u2

libaudiofile-dbg\_0.3.6-2+deb8u2

libaudiofile1\_0.3.6-2+deb8u2

### **130733 - Debian Linux 8.0 DSA-3818-1 Update Is Not Installed**

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2016-9809, CVE-2016-9812, CVE-2016-9813, CVE-2017-5843, CVE-2017-5848

### Description

The scan detected that the host is missing the following update:

DSA-3818-1

### Observation

Updates often remediate critical security problems that should be quickly addressed.

For more information see:

<http://www.debian.org/security/2017/dsa-3818>

Debian 8.0

all

gststreamer1.0-plugins-bad-doc\_1.4.4-2.1+deb8u2

libgststreamer-plugins-bad1.0-dev\_1.4.4-2.1+deb8u2

libgststreamer-plugins-bad1.0-0\_1.4.4-2.1+deb8u2

gststreamer1.0-plugins-bad-dbg\_1.4.4-2.1+deb8u2  
gststreamer1.0-plugins-bad\_1.4.4-2.1+deb8u2

### 163305 - Oracle Enterprise Linux ELSA-2017-0565 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Oracle Enterprise Linux Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2015-8869

#### Description

The scan detected that the host is missing the following update:  
ELSA-2017-0565

#### Observation

Updates often remediate critical security problems that should be quickly addressed.  
For more information see:

<http://oss.oracle.com/pipermail/el-errata/2017-March/006796.html>

#### OEL6

x86\_64

ocaml-labltk-3.11.2-5.el6  
ocaml-emacs-3.11.2-5.el6  
ocaml-ocamldoc-3.11.2-5.el6  
ocaml-x11-3.11.2-5.el6  
ocaml-source-3.11.2-5.el6  
ocaml-runtime-3.11.2-5.el6  
ocaml-3.11.2-5.el6  
ocaml-camlp4-3.11.2-5.el6  
ocaml-camlp4-devel-3.11.2-5.el6  
ocaml-labltk-devel-3.11.2-5.el6  
ocaml-docs-3.11.2-5.el6

i386

ocaml-labltk-3.11.2-5.el6  
ocaml-emacs-3.11.2-5.el6  
ocaml-ocamldoc-3.11.2-5.el6  
ocaml-x11-3.11.2-5.el6  
ocaml-source-3.11.2-5.el6  
ocaml-runtime-3.11.2-5.el6  
ocaml-3.11.2-5.el6  
ocaml-camlp4-3.11.2-5.el6  
ocaml-camlp4-devel-3.11.2-5.el6  
ocaml-labltk-devel-3.11.2-5.el6  
ocaml-docs-3.11.2-5.el6

### 163306 - Oracle Enterprise Linux ELSA-2017-0630 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Oracle Enterprise Linux Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2016-10207, CVE-2017-5581

#### Description

The scan detected that the host is missing the following update:  
ELSA-2017-0630

### Observation

Updates often remediate critical security problems that should be quickly addressed.  
For more information see:

<http://oss.oracle.com/pipermail/el-errata/2017-March/006799.html>

OEL6

x86\_64

tigervnc-server-1.1.0-24.el6

tigervnc-1.1.0-24.el6

tigervnc-server-applet-1.1.0-24.el6

tigervnc-server-module-1.1.0-24.el6

i386

tigervnc-server-1.1.0-24.el6

tigervnc-1.1.0-24.el6

tigervnc-server-applet-1.1.0-24.el6

tigervnc-server-module-1.1.0-24.el6

### **163311 - Oracle Enterprise Linux ELSA-2017-0564 Update Is Not Installed**

Category: SSH Module -> NonIntrusive -> Oracle Enterprise Linux Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2015-8869

### Description

The scan detected that the host is missing the following update:  
ELSA-2017-0564

### Observation

Updates often remediate critical security problems that should be quickly addressed.  
For more information see:

<http://oss.oracle.com/pipermail/el-errata/2017-March/006801.html>

OEL6

x86\_64

libguestfs-devel-1.20.11-20.el6

libguestfs-tools-1.20.11-20.el6

ocaml-libguestfs-1.20.11-20.el6

ocaml-libguestfs-devel-1.20.11-20.el6

libguestfs-java-devel-1.20.11-20.el6

perl-Sys-Guestfs-1.20.11-20.el6

ruby-libguestfs-1.20.11-20.el6

libguestfs-javadoc-1.20.11-20.el6

libguestfs-tools-c-1.20.11-20.el6

libguestfs-1.20.11-20.el6

python-libguestfs-1.20.11-20.el6

libguestfs-java-1.20.11-20.el6

### **163316 - Oracle Enterprise Linux ELSA-2017-0838 Update Is Not Installed**

Category: SSH Module -> NonIntrusive -> Oracle Enterprise Linux Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2016-5139, CVE-2016-5158, CVE-2016-5159, CVE-2016-7163, CVE-2016-9573, CVE-2016-9675

## Description

The scan detected that the host is missing the following update:  
ELSA-2017-0838

## Observation

Updates often remediate critical security problems that should be quickly addressed.  
For more information see:

<http://oss.oracle.com/pipermail/el-errata/2017-March/006791.html>

OEL7  
x86\_64  
openjpeg-1.5.1-16.el7\_3  
openjpeg-libs-1.5.1-16.el7\_3  
openjpeg-devel-1.5.1-16.el7\_3

## 170784 - Amazon Linux AMI ALAS-2017-807 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Amazon Linux Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2016-5139, CVE-2016-5158, CVE-2016-5159, CVE-2016-7163, CVE-2016-9675

## Description

The scan detected that the host is missing the following update:  
ALAS-2017-807

## Observation

Updates often remediate critical security problems that should be quickly addressed.  
For more information see:

<https://alas.aws.amazon.com/ALAS-2017-807.html>

Amazon Linux AMI  
x86\_64  
openjpeg-libs-1.3-16.9.amzn1  
openjpeg-debuginfo-1.3-16.9.amzn1  
openjpeg-1.3-16.9.amzn1  
openjpeg-devel-1.3-16.9.amzn1

i686  
openjpeg-libs-1.3-16.9.amzn1  
openjpeg-1.3-16.9.amzn1  
openjpeg-debuginfo-1.3-16.9.amzn1  
openjpeg-devel-1.3-16.9.amzn1

## 175132 - Scientific Linux Security ERRATA Moderate: openjpeg on SL7.x x86\_64 (1703-9984)

Category: SSH Module -> NonIntrusive -> Scientific Linux Patches and HotFixes

Risk Level: Medium

CVE: CVE-2016-5139, CVE-2016-5158, CVE-2016-5159, CVE-2016-7163, CVE-2016-9573, CVE-2016-9675

## Description

The scan detected that the host is missing the following update:  
Security ERRATA Moderate: openjpeg on SL7.x x86\_64 (1703-9984)

### Observation

Updates often remediate critical security problems that should be quickly addressed.  
For more information see:

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1703&L=scientific-linux-errata&F=&S=&P=9984>

SL7  
x86\_64  
openjpeg-1.5.1-16.el7\_3  
openjpeg-libs-1.5.1-16.el7\_3  
openjpeg-debuginfo-1.5.1-16.el7\_3  
openjpeg-devel-1.5.1-16.el7\_3

### **178419 - Gentoo Linux GLSA-201703-06 Update Is Not Installed**

Category: SSH Module -> NonIntrusive -> Gentoo Linux Patches and HotFixes

Risk Level: Medium

CVE: CVE-2017-7178

### Description

The scan detected that the host is missing the following update:  
GLSA-201703-06

### Observation

Updates often remediate critical security problems that should be quickly addressed.  
For more information see:

<https://security.gentoo.org/glsa/201703-06>

Affected packages:  
net-p2p/deluge < 1.3.14

### **185643 - Ubuntu Linux 14.04 USN-3243-1 Update Is Not Installed**

Category: SSH Module -> NonIntrusive -> Ubuntu Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2014-9938

### Description

The scan detected that the host is missing the following update:  
USN-3243-1

### Observation

Updates often remediate critical security problems that should be quickly addressed.  
For more information see:

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2017-March/003790.html>

Ubuntu 14.04

git\_1.9.1-1ubuntu0.4

### **185644 - Ubuntu Linux 12.04, 14.04 USN-3241-1 Update Is Not Installed**

Category: SSH Module -> NonIntrusive -> Ubuntu Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2017-6827, CVE-2017-6828, CVE-2017-6829, CVE-2017-6830, CVE-2017-6831, CVE-2017-6832, CVE-2017-6833, CVE-2017-6834, CVE-2017-6835, CVE-2017-6836, CVE-2017-6837, CVE-2017-6838, CVE-2017-6839

#### Description

The scan detected that the host is missing the following update:  
USN-3241-1

#### Observation

Updates often remediate critical security problems that should be quickly addressed.  
For more information see:

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2017-March/003788.html>

Ubuntu 12.04

libaudiofile1\_0.3.3-2ubuntu0.3

Ubuntu 14.04

libaudiofile1\_0.3.6-2ubuntu0.14.04.2

### **191872 - Fedora Linux 25 FEDORA-2017-90aaa5bd24 Update Is Not Installed**

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2017-6874

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2017-90aaa5bd24

#### Observation

Updates often remediate critical security problems that should be quickly addressed.  
For more information see:

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/3/?count=200&page=2>

Fedora Core 25

kernel-4.10.5-200.fc25

### **191880 - Fedora Linux 24 FEDORA-2017-15fbaf2450 Update Is Not Installed**

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2017-6874

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2017-15fbaf2450

#### Observation

Updates often remediate critical security problems that should be quickly addressed.

For more information see:

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/3/?count=200&page=1>

Fedora Core 24

kernel-4.9.17-100.fc24

### **21494 - (K53729441) F5 BIG-IP MySQL Vulnerability**

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2016-2047

#### Description

A vulnerability is present in some versions of F5 BIG-IP Products.

#### Observation

F5's BIG-IP product is a network appliance that runs F5's Traffic Management Operating System.

A vulnerability is present in some versions of F5 BIG-IP Products. The flaw lies in the MySQL client libraries. Successful exploitation could allow an attacker to perform man-in-middle attacks or perform unauthorized modifications on the target system. Exploitation requires an F5 BIG-IP appliance with a custom Extended Application Verification (EAV) monitor, using the MySQL client, being executed there.

### **21544 - Cisco Nexus 7000 Series Switches Access-Control Filtering Mechanisms Bypass Vulnerability**

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2017-3875

#### Description

A security bypass vulnerability is present in some versions of Cisco NX-OS Software.

#### Observation

Cisco NX-OS Software is the operating system used in Cisco Nexus devices.

A security bypass vulnerability is present in some versions of Cisco NX-OS Software. The flaw lies in how the affected devices inspect specific traffic when other ACL mechanisms are in use. Successful exploitation could allow an attacker to bypass rules defined on a NTP ACL. Exploitation requires an attacker to send crafted commands for a particular ACL not matched for inspection.

### **21549 - Apache Tomcat Vulnerability Prior To 8.5.11**

Category: General Vulnerability Assessment -> NonIntrusive -> Web Server

Risk Level: Medium

CVE: CVE-2016-8747

#### Description

An information disclosure vulnerability is present in some versions of Apache Tomcat.

#### Observation

Apache Tomcat is a container for the Java Servlet and Java Server Pages Web applications.

An information disclosure vulnerability is present in some versions of Apache Tomcat. The flaw lies in all HTTP connectors and applies when reverse-proxy configurations are enabled. Successful exploitation could allow an attacker to access potentially sensitive information.

### 88852 - Slackware Linux 14.2 SSA:2017-087-01 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Slackware Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2017-3302, CVE-2017-3313

#### Description

The scan detected that the host is missing the following update:  
SSA:2017-087-01

#### Observation

Updates often remediate critical security problems that should be quickly addressed.  
For more information see:

<http://www.slackware.com/security/viewer.php?l=slackware-security&y=2017&m=slackware-security.370121>

Slackware 14.2  
x86\_64  
mariadb-10.0.30-x86\_64-1

i586  
mariadb-10.0.30-i586-1

### 130730 - Debian Linux 8.0 DSA-3815-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2017-6814, CVE-2017-6815, CVE-2017-6816, CVE-2017-6817

#### Description

The scan detected that the host is missing the following update:  
DSA-3815-1

#### Observation

Updates often remediate critical security problems that should be quickly addressed.  
For more information see:

<http://www.debian.org/security/2017/dsa-3815>

Debian 8.0  
all  
wordpress\_4.1+dfsg-1+deb8u13

### 130731 - Debian Linux 8.0 DSA-3822-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2017-5838

#### Description



The scan detected that the host is missing the following update:  
DSA-3822-1

#### Observation

Updates often remediate critical security problems that should be quickly addressed.  
For more information see:

<http://www.debian.org/security/2017/dsa-3822>

Debian 8.0  
all  
libgstreamer1.0-0-dbg\_1.4.4-2+deb8u1  
libgstreamer1.0-dev\_1.4.4-2+deb8u1  
gstreamer1.0-tools\_1.4.4-2+deb8u1  
gstreamer1.0-doc\_1.4.4-2+deb8u1  
libgstreamer1.0-0\_1.4.4-2+deb8u1  
gir1.2-gstreamer-1.0\_1.4.4-2+deb8u1

### 130732 - Debian Linux 8.0 DSA-3820-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2016-10198, CVE-2016-10199, CVE-2017-5840, CVE-2017-5841, CVE-2017-5845

#### Description

The scan detected that the host is missing the following update:  
DSA-3820-1

#### Observation

Updates often remediate critical security problems that should be quickly addressed.  
For more information see:

<http://www.debian.org/security/2017/dsa-3820>

Debian 8.0  
all  
gstreamer1.0-plugins-good-doc\_1.4.4-2+deb8u3  
gstreamer1.0-plugins-good-dbg\_1.4.4-2+deb8u3  
gstreamer1.0-plugins-good\_1.4.4-2+deb8u3  
gstreamer1.0-pulseaudio\_1.4.4-2+deb8u3

### 130734 - Debian Linux 8.0 DSA-3821-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2017-5846, CVE-2017-5847

#### Description

The scan detected that the host is missing the following update:  
DSA-3821-1

#### Observation

Updates often remediate critical security problems that should be quickly addressed.  
For more information see:

<http://www.debian.org/security/2017/dsa-3821>

Debian 8.0

all

gststreamer1.0-plugins-ugly-dbg\_1.4.4-2+deb8u1

gststreamer1.0-plugins-ugly\_1.4.4-2+deb8u1

gststreamer1.0-plugins-ugly-doc\_1.4.4-2+deb8u1

### 130735 - Debian Linux 8.0 DSA-3819-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2016-9811, CVE-2017-5837, CVE-2017-5839, CVE-2017-5842, CVE-2017-5844

#### Description

The scan detected that the host is missing the following update:

DSA-3819-1

#### Observation

Updates often remediate critical security problems that should be quickly addressed.

For more information see:

<http://www.debian.org/security/2017/dsa-3819>

Debian 8.0

all

gststreamer1.0-x\_1.4.4-2+deb8u1

gir1.2-gst-plugins-base-1.0\_1.4.4-2+deb8u1

gststreamer1.0-plugins-base\_1.4.4-2+deb8u1

libgststreamer-plugins-base1.0-0\_1.4.4-2+deb8u1

libgststreamer-plugins-base1.0-dev\_1.4.4-2+deb8u1

gststreamer1.0-alsa\_1.4.4-2+deb8u1

gststreamer1.0-plugins-base-dbg\_1.4.4-2+deb8u1

gststreamer1.0-plugins-base-doc\_1.4.4-2+deb8u1

gststreamer1.0-plugins-base-apps\_1.4.4-2+deb8u1

### 145275 - SuSE SLES 12 SP1, 12 SP2 SUSE-SU-2017:0839-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2016-2183

#### Description

The scan detected that the host is missing the following update:

SUSE-SU-2017:0839-1

#### Observation

Updates often remediate critical security problems that should be quickly addressed.

For more information see:

<http://lists.suse.com/pipermail/sle-security-updates/2017-March/002742.html>

SuSE SLES 12 SP1

x86\_64

java-1\_8\_0-ibm-plugin-1.8.0\_sr4.1-26.2

java-1\_8\_0-ibm-1.8.0\_sr4.1-26.2

java-1\_8\_0-ibm-alsa-1.8.0\_sr4.1-26.2

SuSE SLES 12 SP2

x86\_64

java-1\_8\_0-ibm-plugin-1.8.0\_sr4.1-26.2

java-1\_8\_0-ibm-1.8.0\_sr4.1-26.2

java-1\_8\_0-ibm-alsa-1.8.0\_sr4.1-26.2

### 163302 - Oracle Enterprise Linux ELSA-2017-0654 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Oracle Enterprise Linux Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2017-2616

#### Description

The scan detected that the host is missing the following update:

ELSA-2017-0654

#### Observation

Updates often remediate critical security problems that should be quickly addressed.

For more information see:

<http://oss.oracle.com/pipermail/el-errata/2017-March/006811.html>

OEL6

x86\_64

coreutils-libs-8.4-46.0.1.el6

coreutils-8.4-46.0.1.el6

i386

coreutils-libs-8.4-46.0.1.el6

coreutils-8.4-46.0.1.el6

### 163308 - Oracle Enterprise Linux ELSA-2017-0744 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Oracle Enterprise Linux Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2016-2125, CVE-2016-2126

#### Description

The scan detected that the host is missing the following update:

ELSA-2017-0744

#### Observation

Updates often remediate critical security problems that should be quickly addressed.

For more information see:

<http://oss.oracle.com/pipermail/el-errata/2017-March/006804.html>

OEL6

x86\_64

samba4-dc-libs-4.2.10-9.el6

samba4-test-4.2.10-9.el6

samba4-devel-4.2.10-9.el6

samba4-winbind-krb5-locator-4.2.10-9.el6

samba4-common-4.2.10-9.el6

samba4-winbind-4.2.10-9.el6  
samba4-client-4.2.10-9.el6  
samba4-winbind-clients-4.2.10-9.el6  
samba4-dc-4.2.10-9.el6  
samba4-pidl-4.2.10-9.el6  
samba4-libs-4.2.10-9.el6  
samba4-python-4.2.10-9.el6  
samba4-4.2.10-9.el6

i386

samba4-dc-libs-4.2.10-9.el6  
samba4-test-4.2.10-9.el6  
samba4-devel-4.2.10-9.el6  
samba4-winbind-krb5-locator-4.2.10-9.el6  
samba4-common-4.2.10-9.el6  
samba4-winbind-4.2.10-9.el6  
samba4-client-4.2.10-9.el6  
samba4-winbind-clients-4.2.10-9.el6  
samba4-dc-4.2.10-9.el6  
samba4-pidl-4.2.10-9.el6  
samba4-libs-4.2.10-9.el6  
samba4-python-4.2.10-9.el6  
samba4-4.2.10-9.el6

#### 178416 - Gentoo Linux GLSA-201703-04 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Gentoo Linux Patches and HotFixes

Risk Level: Medium

CVE: CVE-2017-2629

##### Description

The scan detected that the host is missing the following update:  
GLSA-201703-04

##### Observation

Updates often remediate critical security problems that should be quickly addressed.  
For more information see:

<https://security.gentoo.org/glsa/201703-04>

Affected packages:

net-misc/curl < 7.53.0

#### 178417 - Gentoo Linux GLSA-201703-07 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Gentoo Linux Patches and HotFixes

Risk Level: Medium

CVE: CVE-2017-2620

##### Description

The scan detected that the host is missing the following update:  
GLSA-201703-07

##### Observation

Updates often remediate critical security problems that should be quickly addressed.  
For more information see:

<https://security.gentoo.org/glsa/201703-07>

Affected packages:

app-emulation/xen-tools < 4.7.1-r8

### 185637 - Ubuntu Linux 12.04, 14.04, 16.04, 16.10 USN-3244-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Ubuntu Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2016-9811, CVE-2017-5837, CVE-2017-5839, CVE-2017-5842, CVE-2017-5844

#### Description

The scan detected that the host is missing the following update:

USN-3244-1

#### Observation

Updates often remediate critical security problems that should be quickly addressed.

For more information see:

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2017-March/003793.html>

Ubuntu 12.04

gststreamer0.10-plugins-base\_0.10.36-1ubuntu0.2

Ubuntu 16.04

gststreamer1.0-plugins-base\_1.8.3-1ubuntu0.2

Ubuntu 14.04

gststreamer1.0-plugins-base\_1.2.4-1~ubuntu2.1

gststreamer0.10-plugins-base\_0.10.36-1.1ubuntu2.1

Ubuntu 16.10

gststreamer1.0-plugins-base\_1.8.3-1ubuntu1.1

### 185638 - Ubuntu Linux 12.04, 14.04, 16.04, 16.10 USN-3245-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Ubuntu Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2016-10198, CVE-2016-10199, CVE-2017-5840, CVE-2017-5841, CVE-2017-5845

#### Description

The scan detected that the host is missing the following update:

USN-3245-1

#### Observation

Updates often remediate critical security problems that should be quickly addressed.

For more information see:

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2017-March/003794.html>

Ubuntu 12.04

gststreamer0.10-plugins-good\_0.10.31-1ubuntu1.5

Ubuntu 16.04

gststreamer1.0-plugins-good\_1.8.3-1ubuntu0.4

Ubuntu 14.04

gststreamer1.0-plugins-good\_1.2.4-1~ubuntu1.4  
gststreamer0.10-plugins-good\_0.10.31-3+nmu1ubuntu5.3

Ubuntu 16.10

gststreamer1.0-plugins-good\_1.8.3-1ubuntu1.3

### 191864 - Fedora Linux 25 FEDORA-2017-340718eb7b Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2017-6318

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2017-340718eb7b

#### Observation

Updates often remediate critical security problems that should be quickly addressed.  
For more information see:

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/3/?count=200&page=3>

Fedora Core 25

sane-backends-1.0.25-7.fc25

### 88854 - Slackware Linux 14.0, 14.1, 14.2 SSA:2017-082-01 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Slackware Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2017-5604

#### Description

The scan detected that the host is missing the following update:  
SSA:2017-082-01

#### Observation

Updates often remediate critical security problems that should be quickly addressed.  
For more information see:

<http://www.slackware.com/security/viewer.php?l=slackware-security&y=2017&m=slackware-security.438176>

Slackware 14.0

x86\_64

mcabber-1.0.5-x86\_64-1

Slackware 14.2  
x86\_64  
mcabber-1.0.5-x86\_64-1

i586  
mcabber-1.0.5-i586-1

Slackware 14.1  
x86\_64  
mcabber-1.0.5-x86\_64-1

### 141527 - Red Hat Enterprise Linux RHSA-2017-0837 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Red Hat Enterprise Linux Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2017-5208, CVE-2017-5332, CVE-2017-5333, CVE-2017-6009, CVE-2017-6010, CVE-2017-6011

#### Description

The scan detected that the host is missing the following update:

RHSA-2017-0837

#### Observation

Updates often remediate critical security problems that should be quickly addressed.

For more information see:

<https://rhn.redhat.com/errata/RHSA-2017-0837.html>

RHEL7D  
x86\_64  
icoutils-debuginfo-0.31.3-1.el7\_3  
icoutils-0.31.3-1.el7\_3

RHEL7S  
x86\_64  
icoutils-debuginfo-0.31.3-1.el7\_3  
icoutils-0.31.3-1.el7\_3

RHEL7WS  
x86\_64  
icoutils-debuginfo-0.31.3-1.el7\_3  
icoutils-0.31.3-1.el7\_3

### 145271 - SuSE SLES 11 SP4 SUSE-SU-2017:0799-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2017-6508

#### Description

The scan detected that the host is missing the following update:

SUSE-SU-2017:0799-1

#### Observation

Updates often remediate critical security problems that should be quickly addressed.

For more information see:

<http://lists.suse.com/pipermail/sle-security-updates/2017-March/002739.html>

SuSE SLES 11 SP4  
i586  
wget-1.11.4-1.40.1

x86\_64  
wget-1.11.4-1.40.1

### 145273 - SuSE SLES 12 SP1, 12 SP2, SLED 12 SP1, 12 SP2 SUSE-SU-2017:0800-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2017-6508

#### Description

The scan detected that the host is missing the following update:

SUSE-SU-2017:0800-1

#### Observation

Updates often remediate critical security problems that should be quickly addressed.

For more information see:

<http://lists.suse.com/pipermail/sle-security-updates/2017-March/002740.html>

SuSE SLED 12 SP1  
x86\_64  
wget-debuginfo-1.14-20.1  
wget-1.14-20.1  
wget-debugsource-1.14-20.1

SuSE SLES 12 SP2  
x86\_64  
wget-debuginfo-1.14-20.1  
wget-1.14-20.1  
wget-debugsource-1.14-20.1

SuSE SLED 12 SP2  
x86\_64  
wget-debuginfo-1.14-20.1  
wget-1.14-20.1  
wget-debugsource-1.14-20.1

SuSE SLES 12 SP1  
x86\_64  
wget-debuginfo-1.14-20.1  
wget-1.14-20.1  
wget-debugsource-1.14-20.1

### 145276 - SuSE SLES 12 SP2, SLED 12 SP2 SUSE-SU-2017:0798-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2016-10163, CVE-2016-10214, CVE-2017-5580, CVE-2017-5937, CVE-2017-5956, CVE-2017-5957, CVE-2017-5993, CVE-2017-5994, CVE-2017-6209, CVE-2017-6210, CVE-2017-6317, CVE-2017-6355, CVE-2017-6386

#### Description



The scan detected that the host is missing the following update:  
SUSE-SU-2017:0798-1

#### Observation

Updates often remediate critical security problems that should be quickly addressed.  
For more information see:

<http://lists.suse.com/pipermail/sle-security-updates/2017-March/002738.html>

SuSE SLED 12 SP2  
x86\_64  
virglrenderer-debugsource-0.5.0-11.1  
libvirglrenderer0-0.5.0-11.1  
libvirglrenderer0-debuginfo-0.5.0-11.1

SuSE SLES 12 SP2  
x86\_64  
virglrenderer-debugsource-0.5.0-11.1  
libvirglrenderer0-0.5.0-11.1  
libvirglrenderer0-debuginfo-0.5.0-11.1

### **163303 - Oracle Enterprise Linux ELSA-2017-0837 Update Is Not Installed**

Category: SSH Module -> NonIntrusive -> Oracle Enterprise Linux Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2017-5208, CVE-2017-5332, CVE-2017-5333, CVE-2017-6009, CVE-2017-6010, CVE-2017-6011

#### Description

The scan detected that the host is missing the following update:  
ELSA-2017-0837

#### Observation

Updates often remediate critical security problems that should be quickly addressed.  
For more information see:

<http://oss.oracle.com/pipermail/el-errata/2017-March/006792.html>

OEL7  
x86\_64  
icoutils-0.31.3-1.el7\_3

### **175133 - Scientific Linux Security ERRATA Important: icoutils on SL7.x x86\_64 (1703-9570)**

Category: SSH Module -> NonIntrusive -> Scientific Linux Patches and HotFixes

Risk Level: Medium

CVE: CVE-2017-5208, CVE-2017-5332, CVE-2017-5333, CVE-2017-6009, CVE-2017-6010, CVE-2017-6011

#### Description

The scan detected that the host is missing the following update:  
Security ERRATA Important: icoutils on SL7.x x86\_64 (1703-9570)

#### Observation

Updates often remediate critical security problems that should be quickly addressed.  
For more information see:

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1703&L=scientific-linux-errata&F=&S=&P=9570>

SL7  
x86\_64  
icoutils-debuginfo-0.31.3-1.el7\_3  
icoutils-0.31.3-1.el7\_3

### 178418 - Gentoo Linux GLSA-201703-05 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Gentoo Linux Patches and HotFixes

Risk Level: Medium

CVE: CVE-2016-4008

#### Description

The scan detected that the host is missing the following update:

GLSA-201703-05

#### Observation

Updates often remediate critical security problems that should be quickly addressed.

For more information see:

<https://security.gentoo.org/glsa/201703-05>

Affected packages:

dev-libs/libtasn1 < 4.8

### 88853 - Slackware Linux 14.0, 14.1, 14.2 SSA:2017-082-02 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Slackware Patches and Hotfixes

Risk Level: Low

CVE: CVE-2017-2619

#### Description

The scan detected that the host is missing the following update:

SSA:2017-082-02

#### Observation

Updates often remediate critical security problems that should be quickly addressed.

For more information see:

<http://www.slackware.com/security/viewer.php?l=slackware-security&y=2017&m=slackware-security.435262>

Slackware 14.0  
x86\_64  
samba-4.4.12-x86\_64-1

Slackware 14.2  
x86\_64  
samba-4.4.12-x86\_64-1

i586  
samba-4.4.12-i586-1

Slackware 14.1  
x86\_64  
samba-4.4.12-x86\_64-1

### 130727 - Debian Linux 8.0 DSA-3816-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes

Risk Level: Low

CVE: CVE-2017-2619

#### Description

The scan detected that the host is missing the following update:  
DSA-3816-1

#### Observation

Updates often remediate critical security problems that should be quickly addressed.  
For more information see:

<http://www.debian.org/security/2017/dsa-3816>

Debian 8.0  
all  
samba\_2:4.2.14+dfsg-0+deb8u4

### 130729 - Debian Linux 8.0 DSA-3823-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes

Risk Level: Low

CVE: CVE-2017-6964

#### Description

The scan detected that the host is missing the following update:  
DSA-3823-1

#### Observation

Updates often remediate critical security problems that should be quickly addressed.  
For more information see:

<http://www.debian.org/security/2017/dsa-3823>

Debian 8.0  
all  
eject\_2.1.5+deb1+cvs20081104-13.1+deb8u1

### 130736 - Debian Linux 8.0 DSA-3817-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes

Risk Level: Low

CVE: CVE-2016-9601

#### Description

The scan detected that the host is missing the following update:  
DSA-3817-1

#### Observation

Updates often remediate critical security problems that should be quickly addressed.  
For more information see:

<http://www.debian.org/security/2017/dsa-3817>

Debian 8.0  
all  
jbig2dec\_0.13-4~deb8u1

### 170783 - Amazon Linux AMI ALAS-2017-806 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Amazon Linux Patches and Hotfixes

Risk Level: Low

CVE: CVE-2016-9586

#### Description

The scan detected that the host is missing the following update:

ALAS-2017-806

#### Observation

Updates often remediate critical security problems that should be quickly addressed.

For more information see:

<https://alas.aws.amazon.com/ALAS-2017-806.html>

Amazon Linux AMI

x86\_64

libcurl-7.47.1-9.70.amzn1

libcurl-devel-7.47.1-9.70.amzn1

curl-debuginfo-7.47.1-9.70.amzn1

curl-7.47.1-9.70.amzn1

i686

libcurl-7.47.1-9.70.amzn1

libcurl-devel-7.47.1-9.70.amzn1

curl-debuginfo-7.47.1-9.70.amzn1

curl-7.47.1-9.70.amzn1

### 182314 - FreeBSD hostapd Multiple Vulnerabilities (04bc4e23-9a70-42cb-9fec-3613632d34bc)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes

Risk Level: Low

CVE: CVE-MAP-NOMATCH

#### Description

The scan detected that the host is missing the following update:

hostapd -- multiple vulnerabilities (04bc4e23-9a70-42cb-9fec-3613632d34bc)

#### Observation

Updates often remediate critical security problems that should be quickly addressed.

For more information see:

<http://www.vuxml.org/freebsd/04bc4e23-9a70-42cb-9fec-3613632d34bc.html>

Affected packages:

hostapd < 2.6

## 182315 - FreeBSD xen-tools Cirrus VGA Heap Overflow Via Display Refresh (af19ecd0-0f6a-11e7-970f-002590263bf5)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes

Risk Level: Low

CVE: CVE-2016-9603

### Description

The scan detected that the host is missing the following update:

xen-tools -- Cirrus VGA Heap overflow via display refresh (af19ecd0-0f6a-11e7-970f-002590263bf5)

### Observation

Updates often remediate critical security problems that should be quickly addressed.

For more information see:

<http://www.vuxml.org/freebsd/af19ecd0-0f6a-11e7-970f-002590263bf5.html>

Affected packages:

xen-tools < 4.7.2

## 182316 - FreeBSD samba Symlink Race Allows Access Outside Share Definition (2826317b-10ec-11e7-944e-000c292e4fd8)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes

Risk Level: Low

CVE: CVE-2017-2619

### Description

The scan detected that the host is missing the following update:

samba -- symlink race allows access outside share definition (2826317b-10ec-11e7-944e-000c292e4fd8)

### Observation

Updates often remediate critical security problems that should be quickly addressed.

For more information see:

<http://www.vuxml.org/freebsd/2826317b-10ec-11e7-944e-000c292e4fd8.html>

Affected packages:

3.6.0 <= samba36 <= 3.6.25\_4

4.0.0 <= samba4 <= 4.0.26

4.1.0 <= samba41 <= 4.1.23

4.2.0 <= samba42 <= 4.2.14

4.3.0 <= samba43 <= 4.3.13

4.4.0 <= samba44 < 4.4.12

4.5.0 <= samba45 < 4.5.7

4.6.0 <= samba46 < 4.6.1

## 185639 - Ubuntu Linux 12.04, 14.04, 16.04, 16.10 USN-3246-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Ubuntu Patches and Hotfixes

Risk Level: Low

CVE: CVE-2017-6964

### Description

The scan detected that the host is missing the following update:

USN-3246-1

### Observation

Updates often remediate critical security problems that should be quickly addressed.  
For more information see:

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2017-March/003795.html>

Ubuntu 12.04

eject\_2.1.5+deb1+cvs20081104-9ubuntu0.1

Ubuntu 16.04

eject\_2.1.5+deb1+cvs20081104-13.1ubuntu0.16.04.1

Ubuntu 14.04

eject\_2.1.5+deb1+cvs20081104-13.1ubuntu0.14.04.1

Ubuntu 16.10

eject\_2.1.5+deb1+cvs20081104-13.1ubuntu0.16.10.1

### **185640 - Ubuntu Linux 12.04, 14.04, 16.04, 16.10 USN-3247-1 Update Is Not Installed**

Category: SSH Module -> NonIntrusive -> Ubuntu Patches and Hotfixes

Risk Level: Low

CVE: CVE-2017-6507

### Description

The scan detected that the host is missing the following update:  
USN-3247-1

### Observation

Updates often remediate critical security problems that should be quickly addressed.  
For more information see:

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2017-March/003796.html>

Ubuntu 12.04

apparmor\_2.7.102-0ubuntu3.11

Ubuntu 16.04

apparmor\_2.10.95-0ubuntu2.6

Ubuntu 14.04

apparmor\_2.10.95-0ubuntu2.6~14.04.1

Ubuntu 16.10

apparmor\_2.10.95-4ubuntu5.3

### **185641 - Ubuntu Linux 12.04, 14.04, 16.04, 16.10 USN-3242-1 Update Is Not Installed**

Category: SSH Module -> NonIntrusive -> Ubuntu Patches and Hotfixes

Risk Level: Low

CVE: CVE-2017-2619

### Description

The scan detected that the host is missing the following update:  
USN-3242-1

### Observation

Updates often remediate critical security problems that should be quickly addressed.  
For more information see:

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2017-March/003789.html>

Ubuntu 12.04

samba\_3.6.25-0ubuntu0.12.04.9

Ubuntu 16.04

samba\_4.3.11+dfsg-0ubuntu0.16.04.5

Ubuntu 14.04

samba\_4.3.11+dfsg-0ubuntu0.14.04.6

Ubuntu 16.10

samba\_4.4.5+dfsg-2ubuntu5.4

## **185645 - Ubuntu Linux 12.04, 14.04, 16.04, 16.10 USN-3233-1 Update Is Not Installed**

Category: SSH Module -> NonIntrusive -> Ubuntu Patches and Hotfixes

Risk Level: Low

CVE: CVE-2017-5398, CVE-2017-5400, CVE-2017-5401, CVE-2017-5402, CVE-2017-5404, CVE-2017-5405, CVE-2017-5407, CVE-2017-5408, CVE-2017-5410

### Description

The scan detected that the host is missing the following update:  
USN-3233-1

### Observation

Updates often remediate critical security problems that should be quickly addressed.  
For more information see:

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2017-March/003792.html>

Ubuntu 12.04

thunderbird\_45.8.0+build1-0ubuntu0.12.04.1

Ubuntu 16.04

thunderbird\_45.8.0+build1-0ubuntu0.16.04.1

Ubuntu 14.04

thunderbird\_45.8.0+build1-0ubuntu0.14.04.1

Ubuntu 16.10

thunderbird\_45.8.0+build1-0ubuntu0.16.10.1

#### **191863 - Fedora Linux 24 FEDORA-2017-05010f0b46 Update Is Not Installed**

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Low

CVE: CVE-MAP-NOMATCH

##### Description

The scan detected that the host is missing the following update:

FEDORA-2017-05010f0b46

##### Observation

Updates often remediate critical security problems that should be quickly addressed.

For more information see:

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/3/?count=200&page=2>

Fedora Core 24

drupal8-8.2.7-1.fc24

#### **191865 - Fedora Linux 24 FEDORA-2017-922652dd9c Update Is Not Installed**

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Low

CVE: CVE-2017-2784

##### Description

The scan detected that the host is missing the following update:

FEDORA-2017-922652dd9c

##### Observation

Updates often remediate critical security problems that should be quickly addressed.

For more information see:

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/3/?count=200&page=3>

Fedora Core 24

mbdts-2.4.2-1.fc24

#### **191866 - Fedora Linux 25 FEDORA-2017-bd15ca5490 Update Is Not Installed**

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Low

CVE: CVE-MAP-NOMATCH

##### Description

The scan detected that the host is missing the following update:

FEDORA-2017-bd15ca5490



### Observation

Updates often remediate critical security problems that should be quickly addressed.  
For more information see:

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/3/?count=200&page=3>

Fedora Core 25

empathy-3.12.13-2.fc25

### **191867 - Fedora Linux 25 FEDORA-2017-5ebac1c112 Update Is Not Installed**

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Low

CVE: CVE-2017-6451, CVE-2017-6458, CVE-2017-6462, CVE-2017-6463, CVE-2017-6464

### Description

The scan detected that the host is missing the following update:  
FEDORA-2017-5ebac1c112

### Observation

Updates often remediate critical security problems that should be quickly addressed.  
For more information see:

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/3/?count=200&page=1>

Fedora Core 25

ntp-4.2.6p5-44.fc25

### **191868 - Fedora Linux 25 FEDORA-2017-9801754fd7 Update Is Not Installed**

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Low

CVE: CVE-MAP-NOMATCH

### Description

The scan detected that the host is missing the following update:  
FEDORA-2017-9801754fd7

### Observation

Updates often remediate critical security problems that should be quickly addressed.  
For more information see:

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/3/?count=200&page=1>

Fedora Core 25

drupal8-8.2.7-1.fc25

### **191869 - Fedora Linux 25 FEDORA-2017-cd33654294 Update Is Not Installed**

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Low

CVE: CVE-2017-5428

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2017-cd33654294

#### Observation

Updates often remediate critical security problems that should be quickly addressed.  
For more information see:

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/3/?count=200&page=3>

Fedora Core 25

firefox-52.0-6.fc25

### **191871 - Fedora Linux 25 FEDORA-2017-25ffd5b236 Update Is Not Installed**

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Low

CVE: CVE-MAP-NOMATCH

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2017-25ffd5b236

#### Observation

Updates often remediate critical security problems that should be quickly addressed.  
For more information see:

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/3/?count=200&page=1>

Fedora Core 25

webkitgtk4-2.16.0-1.fc25

### **191873 - Fedora Linux 24 FEDORA-2017-9e1ccfe586 Update Is Not Installed**

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Low

CVE: CVE-2017-5428

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2017-9e1ccfe586

#### Observation

Updates often remediate critical security problems that should be quickly addressed.  
For more information see:

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/3/?count=200&page=1>

Fedora Core 24

### 191874 - Fedora Linux 25 FEDORA-2017-837115524e Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Low

CVE: CVE-MAP-NOMATCH

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2017-837115524e

#### Observation

Updates often remediate critical security problems that should be quickly addressed.  
For more information see:

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/3/?count=200&page=3>

Fedora Core 25

cloud-init-0.7.8-6.fc25

### 191875 - Fedora Linux 24 FEDORA-2017-0f38995622 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Low

CVE: CVE-MAP-NOMATCH

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2017-0f38995622

#### Observation

Updates often remediate critical security problems that should be quickly addressed.  
For more information see:

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/3/?count=200&page=1>

Fedora Core 24

webkitgtk4-2.16.0-1.fc24

### 191876 - Fedora Linux 24 FEDORA-2017-66593c367e Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Low

CVE: CVE-MAP-NOMATCH

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2017-66593c367e

#### Observation

Updates often remediate critical security problems that should be quickly addressed.  
For more information see:

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/3/?count=200&page=1>

Fedora Core 24

qbittorrent-3.3.11-2.fc24

### 191877 - Fedora Linux 25 FEDORA-2017-9ed1b89530 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Low

CVE: CVE-2017-2784

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2017-9ed1b89530

#### Observation

Updates often remediate critical security problems that should be quickly addressed.  
For more information see:

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/3/?count=200&page=3>

Fedora Core 25

mbdts-2.4.2-1.fc25

### 191878 - Fedora Linux 25 FEDORA-2017-b72cafa5b4 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Low

CVE: CVE-2016-10243

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2017-b72cafa5b4

#### Observation

Updates often remediate critical security problems that should be quickly addressed.  
For more information see:

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/3/?count=200&page=1>

Fedora Core 25

texlive-2016-33.20160520.fc25

## ENHANCED CHECKS

The following checks have been updated. Enhancements may include optimizations, changes that reflect new information on a vulnerability and anything else that improves upon an existing FSL check.

### 144131 - SuSE Linux 13.2 openSUSE-SU-2016:0065-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: High

CVE: CVE-2015-0855

[Update Details](#)

Risk is updated

### 181857 - FreeBSD pitivi Code Execution (6540c8f0-dca3-11e5-8fa8-14dae9d210b8)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes

Risk Level: High

CVE: CVE-2015-0855

[Update Details](#)

Risk is updated

### 190207 - Fedora Linux 22 FEDORA-2016-cbb76d0e3a Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: High

CVE: CVE-2015-0855

[Update Details](#)

Risk is updated

### 33185 - Oracle Solaris 118667-34 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Solaris Patches and Hotfixes

Risk Level: High

CVE: CVE-2008-2086, CVE-2009-3910

[Update Details](#)

Name is updated Description is updated Observation is updated Recommendation is updated FASLScript is updated

### 33201 - Oracle Solaris 118666-34 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Solaris Patches and Hotfixes

Risk Level: High

CVE: CVE-2008-2086, CVE-2009-3910

[Update Details](#)

Name is updated Description is updated Observation is updated Recommendation is updated FASLScript is updated

### 33217 - Oracle Solaris 118668-34 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Solaris Patches and Hotfixes

Risk Level: High

CVE: CVE-2008-2086, CVE-2009-3910

[Update Details](#)

Name is updated Description is updated Observation is updated Recommendation is updated FASLScript is updated

### 33219 - Oracle Solaris 118669-34 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Solaris Patches and Hotfixes

Risk Level: High

CVE: CVE-2008-2086, CVE-2009-3910

#### Update Details

Name is updated Description is updated Observation is updated Recommendation is updated FASLScript is updated

### 130724 - Debian Linux 8.0 DSA-3812-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes

Risk Level: High

CVE: CVE-2017-6903

#### Update Details

Risk is updated

### 88839 - Slackware Linux 14.0, 14.1, 14.2 SSA:2017-011-02 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Slackware Patches and Hotfixes

Risk Level: High

CVE: CVE-2017-5334, CVE-2017-5335, CVE-2017-5336, CVE-2017-5337

#### Update Details

Risk is updated

### 141522 - Red Hat Enterprise Linux RHSA-2017-0574 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Red Hat Enterprise Linux Patches and Hotfixes

Risk Level: High

CVE: CVE-2016-8610, CVE-2017-5335, CVE-2017-5336, CVE-2017-5337

#### Update Details

Risk is updated

### 170781 - Amazon Linux AMI ALAS-2017-805 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Amazon Linux Patches and Hotfixes

Risk Level: High

CVE: CVE-2016-7097, CVE-2017-5551, CVE-2017-5897, CVE-2017-5970, CVE-2017-5986, CVE-2017-6074

#### Update Details

CVE is updated

### 178385 - Gentoo Linux GLSA-201702-04 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Gentoo Linux Patches and HotFixes

Risk Level: High

CVE: CVE-2017-5334, CVE-2017-5335, CVE-2017-5336, CVE-2017-5337

[Update Details](#)

Risk is updated

**191611 - Fedora Linux 25 FEDORA-2017-2ddf7d452a Update Is Not Installed**

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: High

CVE: CVE-2016-10128, CVE-2016-10129, CVE-2016-10130, CVE-2017-5338, CVE-2017-5339

[Update Details](#)

Risk is updated

**191616 - Fedora Linux 24 FEDORA-2017-403346d884 Update Is Not Installed**

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: High

CVE: CVE-2016-10128, CVE-2016-10129, CVE-2016-10130, CVE-2017-5338, CVE-2017-5339

[Update Details](#)

Risk is updated

**191624 - Fedora Linux 24 FEDORA-2017-e86817c42e Update Is Not Installed**

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: High

CVE: CVE-2017-5334, CVE-2017-5335, CVE-2017-5336, CVE-2017-5337

[Update Details](#)

Risk is updated

**191716 - Fedora Linux 24 FEDORA-2017-92d84f68cf Update Is Not Installed**

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: High

CVE: CVE-2017-5897

[Update Details](#)

Risk is updated

**20925 - Apache Tomcat Multiple Vulnerabilities Prior To 8.5.8**

Category: General Vulnerability Assessment -> NonIntrusive -> Web Server

Risk Level: Medium

CVE: CVE-2016-6816, CVE-2016-6817, CVE-2016-8735

[Update Details](#)

Risk is updated

**130650 - Debian Linux 8.0 DSA-3738-1 Update Is Not Installed**

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2016-6816, CVE-2016-8735, CVE-2016-9774, CVE-2016-9775

[Update Details](#)

Risk is updated

#### **130651 - Debian Linux 8.0 DSA-3739-1 Update Is Not Installed**

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2016-6816, CVE-2016-8735, CVE-2016-9774, CVE-2016-9775

[Update Details](#)

Risk is updated

#### **141511 - Red Hat Enterprise Linux RHSA-2017-0527 Update Is Not Installed**

Category: SSH Module -> NonIntrusive -> Red Hat Enterprise Linux Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2016-6816, CVE-2016-8745

[Update Details](#)

Risk is updated

#### **145060 - SuSE SLES 12 SP1 SUSE-SU-2016:3079-1 Update Is Not Installed**

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2016-0762, CVE-2016-5018, CVE-2016-6794, CVE-2016-6796, CVE-2016-6797, CVE-2016-6816, CVE-2016-8735

[Update Details](#)

Risk is updated

#### **145063 - SuSE SLES 12 SP2 SUSE-SU-2016:3081-1 Update Is Not Installed**

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2016-0762, CVE-2016-5018, CVE-2016-6794, CVE-2016-6796, CVE-2016-6797, CVE-2016-6816, CVE-2016-8735

[Update Details](#)

Risk is updated

#### **160226 - CentOS 6 CESA-2017-0527 Update Is Not Installed**

Category: SSH Module -> NonIntrusive -> Cent OS Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2016-6816, CVE-2016-8745

[Update Details](#)



Risk is updated

#### **163300 - Oracle Enterprise Linux ELSA-2017-0527 Update Is Not Installed**

Category: SSH Module -> NonIntrusive -> Oracle Enterprise Linux Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2016-6816, CVE-2016-8745

[Update Details](#)

Risk is updated

#### **170750 - Amazon Linux AMI ALAS-2016-776 Update Is Not Installed**

Category: SSH Module -> NonIntrusive -> Amazon Linux Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2016-6816, CVE-2016-8735

[Update Details](#)

Risk is updated

#### **170751 - Amazon Linux AMI ALAS-2016-777 Update Is Not Installed**

Category: SSH Module -> NonIntrusive -> Amazon Linux Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2016-6816, CVE-2016-8735

[Update Details](#)

Risk is updated

#### **170755 - Amazon Linux AMI ALAS-2016-778 Update Is Not Installed**

Category: SSH Module -> NonIntrusive -> Amazon Linux Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2016-6816, CVE-2016-8735

[Update Details](#)

Risk is updated

#### **175129 - Scientific Linux Security ERRATA Moderate: tomcat6 on SL6.x (noarch) (1703-8501)**

Category: SSH Module -> NonIntrusive -> Scientific Linux Patches and HotFixes

Risk Level: Medium

CVE: CVE-2016-6816, CVE-2016-8745

[Update Details](#)

Risk is updated

#### **181734 - FreeBSD mediawiki Multiple Vulnerabilities (f36bbd66-aa44-11e5-8f5c-002590263bf5)**

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2015-8622, CVE-2015-8623, CVE-2015-8624, CVE-2015-8625, CVE-2015-8626, CVE-2015-8627, CVE-2015-8628

[Update Details](#)

Risk is updated

**182244 - FreeBSD tomcat Multiple Vulnerabilities (0b9af110-d529-11e6-ae1b-002590263bf5)**

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2016-6816, CVE-2016-8735

[Update Details](#)

Risk is updated

**191514 - Fedora Linux 25 FEDORA-2016-98cca07999 Update Is Not Installed**

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2016-6816, CVE-2016-6817, CVE-2016-8735

[Update Details](#)

Risk is updated

**191515 - Fedora Linux 23 FEDORA-2016-9c33466fbb Update Is Not Installed**

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2016-6816, CVE-2016-6817, CVE-2016-8735

[Update Details](#)

Risk is updated

**191517 - Fedora Linux 24 FEDORA-2016-a98c560116 Update Is Not Installed**

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2016-6816, CVE-2016-6817, CVE-2016-8735

[Update Details](#)

Risk is updated

**130692 - Debian Linux 8.0 DSA-3781-1 Update Is Not Installed**

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2017-5617

[Update Details](#)

Risk is updated

**145091 - SuSE SLES 11 SP4 SUSE-SU-2016:3162-1 Update Is Not Installed**

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2016-7035, CVE-2016-7797

[Update Details](#)

Risk is updated

#### **145257 - SuSE SLES 11 SP4 SUSE-SU-2017:0717-1 Update Is Not Installed**

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2017-6318

[Update Details](#)

Risk is updated

#### **145266 - SuSE SLES 12 SP1, 12 SP2, SLED 12 SP1, 12 SP2 SUSE-SU-2017:0713-1 Update Is Not Installed**

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2017-6318

[Update Details](#)

Risk is updated

#### **181950 - FreeBSD wpa\_supplicant Psk Configuration Parameter Update Allowing Arbitrary Data To Be Written (967b852b-1e28-11e6-8dd3-0025902**

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2016-4476, CVE-2016-4477

[Update Details](#)

FASLScript is updated

#### **191687 - Fedora Linux 25 FEDORA-2017-6382ea8d57 Update Is Not Installed**

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2016-6225

[Update Details](#)

Risk is updated

#### **191695 - Fedora Linux 24 FEDORA-2017-5a823376be Update Is Not Installed**

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2016-6225

[Update Details](#)

Risk is updated

**191846 - Fedora Linux 24 FEDORA-2017-c1bec8972c Update Is Not Installed**

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2016-8654, CVE-2016-9262

[Update Details](#)

Risk is updated

**191858 - Fedora Linux 25 FEDORA-2017-3dba8a70ce Update Is Not Installed**

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2016-8654, CVE-2016-9262

[Update Details](#)

Risk is updated

**2177 - Netsky.a/Netsky.b Detected**

Category: Windows Host Assessment -> Trojans, Backdoors, Viruses, and Malware  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Documentation is updated FASLScript is updated

**181919 - FreeBSD wpa\_supplicant Multiple Vulnerabilities (976567f6-05c5-11e6-94fa-002590263bf5)**

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes

Risk Level: Low

CVE: CVE-2015-5310, CVE-2015-5315, CVE-2015-5316

[Update Details](#)

FASLScript is updated

**182308 - FreeBSD irssi Use-after-free Potential Code Execution (06f931c0-0be0-11e7-b4bf-5404a68ad561)**

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes

Risk Level: Low

CVE: CVE-2017-7191

[Update Details](#)

CVE is updated

**45000 - ShellLogon.fasl3**

Category: General Vulnerability Assessment -> NonIntrusive -> Invalid Category

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

### 70014 - netbios-helpers.fasl3.inc

Category: General Vulnerability Assessment -> NonIntrusive -> Invalid Category

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

### 70041 - rpm.fasl3.inc

Category: General Vulnerability Assessment -> NonIntrusive -> Invalid Category

Risk Level: Informational

CVE: CVE-2001-0923

Update Details

FASLScript is updated

### 70050 - vmware.fasl3.inc

Category: General Vulnerability Assessment -> NonIntrusive -> Invalid Category

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

## HOW TO UPDATE

FS1000 APPLIANCE customers should follow the instructions for Enterprise/Professional customers, below. In addition, we strongly urge all appliance customers to authorize and install any Windows Update critical patches. The appliance will auto-download any critical updates but will wait for your explicit authorization before installing.

FOUNDSTONE ENTERPRISE and PROFESSIONAL customers may obtain these new scripts using the FSUpdate Utility by selecting "FoundScan Update" on the help menu. Make sure that you have a valid FSUpdate username and password. The new vulnerability scripts will be automatically included in your scans if you have selected that option by right-clicking the selected vulnerability category and checking the "Run New Checks" checkbox.

MANAGED SERVICE CUSTOMERS already have the newest update applied to their environment. The new vulnerability scripts will be automatically included when your scans are next scheduled, provided the Run New Scripts option has been turned on.

## MCAFFEE TECHNICAL SUPPORT

ServicePortal: <https://mysupport.mcafee.com/>

Multi-National Phone Support available here:

<http://www.mcafee.com/us/about/contact/index.html>

Non-US customers - Select your country from the list of Worldwide Offices.

This email may contain confidential and privileged material for the sole use of the intended recipient. Any review or distribution by others is strictly prohibited. If you are not the intended recipient please contact the sender and delete all copies.

Copyright 2017 McAfee, Inc.

McAfee is a registered trademark of McAfee, Inc. and/or its affiliates