2016-OCT-19
FSL version 7.5.858

MCAFEE 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

20695 - (SB10170) McAfee Web Gateway Multiple Vulnerabilities

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2016-1762, CVE-2016-1833, CVE-2016-1834, CVE-2016-1835, CVE-2016-1836, CVE-2016-1837, CVE-2016-1838, CVE-2016-1839, CVE-2016-1840, CVE-2016-3627, CVE-2016-3705, CVE-2016-4447, CVE-2016-4448, CVE-2016-4449

Description

Multiple vulnerabilities are present in some versions of McAfee Web Gateway.

Observation

McAfee Web Gateway is a web based security control system designed to prevent web application attacks.

Multiple vulnerabilities are present in some versions of McAfee Web Gateway. The flaws are related to XML parsing and most of them relies on the libxml2 library. Successful exploitation could allow an attacker to retrieve sensitive data, cause a denial of service condition, remotely execute arbitrary code or have other unspecified impact on the target system.

20470 - (VMSA-2016-0012) VMware Photon OS OVA Default Public SSH Key Security Bypass Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2016-5333

Description

Multiple vulnerabilities are present in some versions of VMware Photon OS.

Observation

VMware Photon OS is a linux-based container host used for VMware Platforms.

Multiple vulnerabilities are present in some versions of VMware Photon OS. The flaws lie in the OVA distributions of this product and are due to a public SSH key that was left in the Photon OS build environment. Successful exploitation could allow an attacker to bypass security access restrictions or retrieve sensitive data.

20710 - (HPSBMU03593) HPE System Management Homepage Multiple Vulnerabilities

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

Risk Level: High

CVE: CVE-2007-6750, CVE-2011-4969, CVE-2015-3194, CVE-2015-3195, CVE-2015-3237, CVE-2015-7995, CVE-2015-8035, CVE-2016-0705, CVE-2016-0799, CVE-2016-2015, CVE-2016-2842

Description

Multiple vulnerabilities are present in some versions of HPE System Management Homepage.

Observation

HPE System Management Homepage is a web-based interface that consolidates and simplifies the management of individual ProLiant and Integrity servers.

Multiple vulnerabilities are present in some versions of HPE System Management Homepage. The flaws lie in multiple components. Successful exploitation could allow an attacker to cause a denial of service condition, execute remote code, disclose or modify sensitive information.

20713 - Oracle Java SE Critical Patch Update October 2016

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

Risk Level: High

CVE: CVE-2016-5542, CVE-2016-5554, CVE-2016-5556, CVE-2016-5568, CVE-2016-5573, CVE-2016-5582, CVE-2016-5597

Description

Multiple vulnerabilities are present in some versions of Oracle Java SE.

Observation

Oracle Java SE is used to run Java applications.

Multiple vulnerabilities are present in some versions of Oracle Java SE. The flaws lie in multiple components. Successful exploitation could allow an attacker to obtain sensitive information or execute arbitrary code.

20692 - Google Chrome Multiple Vulnerabilities Prior To 53.0.2785.143

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

Risk Level: High

CVE: CVE-2016-5177, CVE-2016-5178

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 several components. Successful exploitation could allow an attacker to remotely execute arbitrary code.

20693 - Google Chrome Multiple Vulnerabilities Prior To 53.0.2785.143

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2016-5177, CVE-2016-5178

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 several components. Successful exploitation could allow an attacker to remotely execute arbitrary code.

20696 - Cisco IOS Software H323 Message Validation Denial Of Service Vulnerability (CSCux04257)

Category: SSH Module -> NonIntrusive -> Cisco IOS Patches and Hotfixes

Risk Level: High

CVE: CVE-2016-6384

Description

A denial of service vulnerability is present in some versions of Cisco IOS.

Observation

Cisco IOS is an operating system used in Cisco devices.

A denial of service vulnerability is present in some versions of Cisco IOS. The flaw lies in the H.323 subsystem. Successful exploitation could allow an attacker to cause a denial of service condition.

20701 - Cisco IOS Software DNS Forwarder Denial of Service Vulnerability

Category: SSH Module -> NonIntrusive -> Cisco IOS Patches and Hotfixes

Risk Level: High

CVE: CVE-2016-6380

Description

A denial of service vulnerability is present in some versions of Cisco IOS.

Observation

Cisco IOS is an operating system used in Cisco devices.

A denial of service vulnerability is present in some versions of Cisco IOS. The flaw lies in the DNS forwarder functionality. Successful exploitation could allow an attacker to cause a denial of service condition.

20614 - Mozilla Firefox ESR Multiple Vulnerabilities Prior To 45.4

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

Risk Level: High

CVE: CVE-2016-5250, CVE-2016-5257, CVE-2016-5261, CVE-2016-5270, CVE-2016-5272, CVE-2016-5274, CVE-2016-5276, CVE-2016-5277, CVE-2016-5278, CVE-2016-5280, CVE-2016-5281, CVE-2016-5284

Description

Multiple vulnerabilities are present in some versions of Mozilla Firefox ESR.

Observation

Mozilla Firefox ESR is a popular web browser.

Multiple vulnerabilities are present in some versions of Mozilla Firefox ESR. The flaws lie in several components. Successful exploitation could allow an attacker to cause a denial of service condition, conduct spoofing attacks, retrieve sensitive data, remotely execute arbitrary code or have other unspecified impact on the target system.

20619 - Mozilla Firefox ESR Multiple Vulnerabilities Prior To 45.4

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2016-5250, CVE-2016-5257, CVE-2016-5261, CVE-2016-5270, CVE-2016-5272, CVE-2016-5274, CVE-2016-5276, CVE-2016-5277, CVE-2016-5278, CVE-2016-5280, CVE-2016-5281, CVE-2016-5284

Description

Multiple vulnerabilities are present in some versions of Mozilla Firefox ESR.

Observation

Mozilla Firefox ESR is a popular web browser.

Multiple vulnerabilities are present in some versions of Mozilla Firefox ESR. The flaws lie in several components. Successful exploitation could allow an attacker to cause a denial of service condition, conduct spoofing attacks, retrieve sensitive data, remotely execute arbitrary code or have other unspecified impact on the target system.

20656 - NVIDIA Windows Drivers Multiple Vulnerabilities 10-2016

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

Risk Level: High

CVE: CVE-2016-3161, CVE-2016-4959, CVE-2016-4960, CVE-2016-4961, CVE-2016-5025, CVE-2016-5852

Description

Multiple vulnerabilities are present in some versions of the NVIDIA Drivers.

Observation

NVIDIA is a technology company which manufactures graphics processing units.

Multiple vulnerabilities are present in some versions of the NVIDIA Drivers. The flaws occur within multiple components. Successful exploitation could allow an attacker to cause a denial of service or escalate privileges.

20658 - Cisco IOS Software Multicast Routing Denial of Service Vulnerabilities

Category: SSH Module -> NonIntrusive -> Cisco IOS Patches and Hotfixes

Risk Level: High

CVE: CVE-2016-6382, CVE-2016-6392

Description

Multiple denial of service vulnerabilities are present in some versions of Cisco IOS.

Observation

Cisco IOS is an operating system used in Cisco devices.

Multiple denial of service vulnerabilities are present in some versions of Cisco IOS. The flaws lie in the implementations of IPv4 MSDP and IPv6 PIM. Successful exploitation of these vulnerability could lead to a denial of service condition. Exploitation requires these features to be configured in the system.

20700 - Cisco IOS Software Smart Install Memory Leak Vulnerability

Category: SSH Module -> NonIntrusive -> Cisco IOS Patches and Hotfixes

Risk Level: High

CVE: CVE-2016-6385

Description

A denial of service vulnerability is present in some versions of Cisco IOS.

Observation

Cisco IOS is an operating system used in Cisco devices.

A denial of service vulnerability is present in some versions of Cisco IOS. The flaw lies in the Smart Install client feature. Successful exploitation could allow an attacker to cause a denial of service condition.

20702 - Cisco IOS Software Internet Key Exchange Version 1 Fragmentation Denial of Service Vulnerability

Category: SSH Module -> NonIntrusive -> Cisco IOS Patches and Hotfixes

Risk Level: High

CVE: CVE-2016-6381

Description

A denial of service vulnerability is present in some versions of Cisco IOS.

Observation

Cisco IOS is an operating system used in Cisco devices.

A denial of service vulnerability is present in some versions of Cisco IOS. The flaws lies in the Internet Key Exchange version 1 (IKEv1) fragmentation code. Successful exploitation of these vulnerability could lead to a denial of service condition. Exploitation requires these features to be configured in the system.

20703 - (SB10171) McAfee ePolicy Orchestrator Multiple OpenSSL Vulnerabilities

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

Risk Level: High

CVE: CVE-2016-2182, CVE-2016-2183, CVE-2016-6304, CVE-2016-7052

Description

Multiple vulnerabilities are present in some versions of McAfee ePolicy Orchestrator.

Observation

McAfee ePolicy Orchestrator (ePO) is widely acknowledged as the most advanced and scalable security management software.

Multiple vulnerabilities are present in some versions of McAfee ePolicy Orchestrator. The flaws lie in the OpenSSL component. Successful exploitation could allow an attacker to affect integrity and availability.

20707 - (JSA10764) Juniper Junos J-web Cross Site Scripting Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2016-4923

Description

A cross site scripting vulnerability is present in some versions of Juniper Junos.

Observation

Juniper Junos is an operating system used in Juniper devices.

A cross site scripting vulnerability is present in some versions of Juniper Junos. The flaw lies in J-Web component. Successful exploitation could allow an attacker to execute arbitrary script code.

20708 - Cisco IOS Software IP Detail Record Denial of Service Vulnerability

Category: SSH Module -> NonIntrusive -> Cisco IOS Patches and Hotfixes

Risk Level: High

CVE: CVE-2016-6379

Description

A denial of service vulnerability is present in some versions of Cisco IOS.

Observation

Cisco IOS is an operating system used in Cisco devices.

A denial of service vulnerability is present in some versions of Cisco IOS. The flaw lies in improper handling of IPDR packets. Successful exploitation could allow an attacker to cause a denial of service condition.

20621 - (SOL39508724) F5 BIG-IP TMM SSL/TLS Virtual Server Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2016-6907

Description

An Information disclosure 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.

An Information disclosure vulnerability is present in some versions of F5 BIG-IP products. The flaw lies in SSL/TLS CBC ciphers. Successful exploitation could allow an attacker to perform padding oracle attack to exploit TLS padding and calculate the plaintext.

20659 - IBM WebSphere Application Server Java Remote Code Execution Vulnerability (swg21990060)

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

Risk Level: Medium

CVE: CVE-2016-5983

Description

A remote code execution vulnerability is present in some versions of IBM WebSphere Application Server.

Observation

IBM WebSphere Application Server is a server engine for Java EE Web applications.

A remote code execution vulnerability is present in some versions of IBM WebSphere Application Server. The flaw is due to improper handling access control. Successful exploitation could allow a remote attacker to execute arbitrary Java code.

20661 - IBM WebSphere Application Server Liberty Profile Java Remote Code Execution Vulnerability (swg21990060)

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

Risk Level: Medium

CVE: CVE-2016-5983

Description

A remote code execution vulnerability is present in some versions of IBM WebSphere Application Server Liberty Profile.

Observation

IBM WebSphere Application Server Lliberty Profile is a server engine for Java EE Web applications.

A remote code execution vulnerability is present in some versions of IBM WebSphere Application Server Liberty Profile. The flaw is due to improper handling access control. Successful exploitation could allow a remote attacker to execute arbitrary Java code.

20652 - (VMSA-2016-0015) VMware Horizon View Directory Traversal Vulnerability

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

Risk Level: Medium

CVE: CVE-2016-7087

Description

An information disclosure vulnerability is present in some versions of VMware Horizon View.

Observation

VMware Horizon View is a desktop-virtualization product.

An information disclosure vulnerability is present in some versions of VMware Horizon View. The flaw lies in the Horizon View Connection Server component. Successful exploitation could allow an attacker to read arbitrary data and bypass security measures.

20657 - (CTX217430) Citrix License Server Denial Of Service Vulnerability

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

Risk Level: Medium

CVE: CVE-2016-6273

Description

A denial of service vulnerability is present in some versions of Citrix License Server.

Observation

Citrix License Server is a product used to manage Citrix products licenses.

A denial of service vulnerability is present in some versions of Citrix License Server. The flaw lies in the Flexera FlexNet Publisher component. Successful exploitation could allow an attacker to cause a denial of service condition.

20697 - Wireshark Multiple Vulnerabilities Prior To 2.2.1

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Description

Multiple vulnerabilities are present in some versions of Wireshark.

Observation

Wireshark is a network traffic analyzer.

Multiple vulnerabilities are present in some versions of Wireshark. The flaws lie in multiple dissectors. Successful exploitation could allow an attacker to cause a denial of service condition.

20706 - Ruby on Rails Dynamic Render File Upload Remote Code Execution Vulnerability

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

Risk Level: Medium

CVE: CVE-2016-0752

Description

A directory traversal vulnerability is present in some versions of Ruby on Rails.

Observation

Ruby on Rails is a web application development framework.

A directory traversal vulnerability is present in some versions of Ruby on Rails. The flaw lies in dynamic render. Successful exploitation could allow an attacker to obtain sensitive information or execute arbitrary code.

20709 - (JSA10759) Juniper Junos OpenSSL December 2015 Multiple Vulnerabilities

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2015-1794, CVE-2015-3193, CVE-2015-3194, CVE-2015-3195, CVE-2015-3196

Description

Multiple vulnerabilities are present in some versions of Juniper Junos.

Observation

Juniper Junos is an operating system used in Juniper devices.

Multiple vulnerabilities are present in some versions of Juniper Junos. The flaws lie in the OpenSSL component. Successful exploitation could allow an attacker to obtain sensitive data or cause a denial of service.

20620 - (SOL01324833) F5 BIG-IP NTP Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Low

CVE: CVE-2015-8158

Description

A denial of service 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 denial of service vulnerability is present in some versions of F5 BIG-IP products. The flaw lies in the ntpq utility. Successful exploitation could allow an attacker to cause an infinite loop and eventually crash the ntpq client causing a denial of service condition.

20705 - IBM WebSphere Application Server Liberty Cross-Site Scripting Vulnerability

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

Risk Level: Low

CVE: CVE-2016-3042

Description

A Cross-Site-Scripting vulnerability is present in some versions of IBM WebSphere Application Manager Liberty.

Observation

IBM WebSphere Application Server Lliberty is a server engine for Java EE Web applications.

A Cross-Site-Scripting vulnerability is present in some versions of IBM WebSphere Application Manager Liberty. The flaw lies in the OpenID Connect client module. Successful exploitation could allow the disclosure of user credentials.

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.

20640 - (MS16-123) Security Update for Windows Kernel-Mode Drivers (3192892)

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

Risk Level: High

CVE: CVE-2016-3266, CVE-2016-3341, CVE-2016-3376, CVE-2016-7185, CVE-2016-7211

Update Details

Risk is updated

20653 - (APSB16-32) Vulnerabilities In Adobe Flash Player

Category: Windows Host Assessment -> Adobe Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-4273, CVE-2016-4286, CVE-2016-6981, CVE-2016-6982, CVE-2016-6983, CVE-2016-6984, CVE-2016-6985, CVE-2016-6986, CVE-2016-6987, CVE-2016-6989, CVE-2016-6990, CVE-2016-6992

Update Details

Risk is updated

20654 - (APSB16-32) Vulnerabilities In Adobe Flash Player

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2016-4273, CVE-2016-4286, CVE-2016-6981, CVE-2016-6982, CVE-2016-6983, CVE-2016-6984, CVE-2016-6985, CVE-2016-6986, CVE-2016-6987, CVE-2016-6989, CVE-2016-6990, CVE-2016-6992

Update Details

Risk is updated

20678 - (MS16-120) Security Update for Microsoft Graphics Component (3192884)

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

Risk Level: High

CVE: CVE-2016-3209, CVE-2016-3262, CVE-2016-3263, CVE-2016-3270, CVE-2016-3393, CVE-2016-3396, CVE-2016-7182

Update Details

Risk is updated

20679 - (MS16-120) Security Update for Microsoft Graphics Component (3192884)

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2016-3209, CVE-2016-3262, CVE-2016-3263, CVE-2016-3270, CVE-2016-3393, CVE-2016-3396, CVE-2016-7182

Update Details

Risk is updated

191170 - Fedora Linux 25 FEDORA-2016-f3d1f79398 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-7425

Update Details

Risk is updated

9839 - Microsoft Windows Service Isolation Bypass Vulnerability

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-1886

Update Details

Recommendation is updated

20690 - (MS16-126) Internet Explorer Information Disclosure Vulnerability (3196067)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-3298

Update Details

Observation is updated

20647 - (MS16-124) Security Update for Windows Registry (3193227)

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

Risk Level: Medium

CVE: CVE-2016-0070, CVE-2016-0073, CVE-2016-0075, CVE-2016-0079

Update Details

Risk is updated

144915 - SuSE SLES 12 SP1, SLED 12 SP1 SUSE-SU-2016:2476-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-7796

Update Details

Risk is updated

170717 - Amazon Linux AMI ALAS-2016-740 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-6828

Update Details

Risk is updated

191005 - Fedora Linux 24 FEDORA-2016-5e24d8c350 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-6828

Update Details

Risk is updated

191018 - Fedora Linux 23 FEDORA-2016-723350dd75 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-6828

Update Details

Risk is updated

191191 - Fedora Linux 24 FEDORA-2016-c942ed0424 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-7795, CVE-2016-7796

Update Details

Risk is updated

191204 - Fedora Linux 25 FEDORA-2016-894abe29d2 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-7795

Update Details

Risk is updated

191242 - Fedora Linux 24 FEDORA-2016-861b8c46b7 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-7099

Update Details

Risk is updated

191252 - Fedora Linux 25 FEDORA-2016-43ff70c6b1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-7099

Update Details

Risk 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

70087 - hp.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.

MCAFEE 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.