

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

24607 - Rockwell Automation FactoryTalk Services Platform Heap-based Buffer Overflow Vulnerability

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

Risk Level: High

CVE: CVE-2018-18981

Description

A vulnerability is present in some versions of Rockwell Automation FactoryTalk Services Platform.

Observation

Rockwell Automation FactoryTalk Services Platform provides common services to FactoryTalk softwares.

A vulnerability is present in some versions of Rockwell Automation FactoryTalk Services Platform. The flaw lies in memory consumption in service ports. Successful exploitation could allow an attacker to cause a denial of service condition.

24632 - Microsoft Office 365 ProPlus and Office 2019 Jan 2019 Updates

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

Risk Level: Informational

CVE: CVE-2019-0541, CVE-2019-0559, CVE-2019-0560, CVE-2019-0561, CVE-2019-0585

Description

Multiple issues are present in some versions of Microsoft Office 365 ProPlus and Office 2019.

Observation

Microsoft Office 365 ProPlus and Office 2019 are the industry standard productivity suites.

Multiple issues are present in some versions of Microsoft Office 365 ProPlus and Office 2019. The flaws are present in multiple components. Such defects could lead the product to software vulnerabilities, malfunction or unexpected behavior in some of its affected components.

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.

24507 - (MSPT-Dec2018) Microsoft Edge Improperly Accesses Objects in Memory Remote Code Execution (CVE-2018-8634)

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

Risk Level: High
CVE: CVE-2018-8634

Update Details

FASLScript is updated

24577 - (MSPT-Jan2019) Microsoft .NET Framework Information Disclosure (CVE-2019-0545)

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

Risk Level: Medium
CVE: CVE-2019-0545

Update Details

FASLScript is updated

147488 - SuSE Linux 15.0, 42.3 openSUSE-SU-2018:4212-1 Update Is Not Installed

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

Risk Level: Medium
CVE: CVE-2018-19044, CVE-2018-19045, CVE-2018-19046

Update Details

Risk is updated

24303 - Cisco Catalyst 6800 Series Switches ROM Monitor Software Secure Boot Bypass Vulnerability (cisco-sa-20180926-catalyst6800)

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

Risk Level: Medium
CVE: CVE-2018-15370

Update Details

Risk 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.

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 2019 McAfee, Inc.

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