Advisory Alert

Alert Number: AAA20250910 **Date:** September 10, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Sophos	**Critical**	Authentication Bypass Vulnerability
F5	**Critical**	RADIUS Protocol Authentication Vulnerability
Microsoft	**Critical**	Multiple Vulnerabilities
SUSE	**High**	Multiple Vulnerabilities
Citrix	**High**	Authorization Bypass Vulnerability
F5	**High**	RADIUS Protocol Authentication Vulnerability
IBM	**High**	Multiple Vulnerabilities
Ivanti	**High**, **Medium**	Multiple Vulnerabilities
Fortinet	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**Sophos**
Severity	**Critical**
Affected Vulnerability	Authentication Bypass Vulnerability (CVE-2025-10159)
Description	Sophos has released a security update addressing an authentication bypass vulnerability that exists in their products. **CVE-2025-10159** - An authentication bypass vulnerability allows remote attackers to gain administrative privileges on Sophos AP6 Series Wireless Access Points older than firmware version 1.7.2563 (MR7). Sophos advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Sophos AP6 Series Wireless Access Points firmware prior version 1.7.2563 (MR7)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.sophos.com/en-us/security-advisories/sophos-sa-20250909-ap6

Affected Product	**F5**
Severity	**Critical**
Affected Vulnerability	RADIUS Protocol Authentication Vulnerability (CVE-2024-3596)
Description	F5 has released a security update addressing a RADIUS protocol authentication vulnerability that exists in their products. **CVE-2024-3596** - RADIUS Protocol under RFC 2865 is susceptible to forgery attacks by a local attacker who can modify any valid Response (Access-Accept, Access-Reject, or Access-Challenge) to any other response using a chosen-prefix collision attack against MD5 Response Authenticator signature. F5 advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	F5OS-C Versions - 1.6.0 - 1.6.2 F5OS-A Versions - 1.7.0, 1.5.1 - 1.5.2 BIG-IP Next Central Manager Versions - 20.2.0 - 20.3.0 BIG-IQ Centralized Management Versions - 8.2.0 - 8.4.0 BIG-IP (APM) Versions - 17.1.0 - 17.1.1, 16.1.0 - 16.1.5, 15.1.0 - 15.1.10
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://my.f5.com/manage/s/article/K000141008

Affected Product	**Microsoft**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-21907, CVE-2025-54917, CVE-2025-54911, CVE-2025-54114, CVE-2025-54109, CVE-2025-54108, CVE-2025-54107, CVE-2025-54098, CVE-2025-54092, CVE-2025-53808, CVE-2025-53804, CVE-2025-53803, CVE-2025-55236, CVE-2025-55232, CVE-2025-55228, CVE-2025-54919, CVE-2025-54913, CVE-2025-54902, CVE-2025-54899, CVE-2025-54894, CVE-2025-54102, CVE-2025-54096, CVE-2025-55234, CVE-2025-55227, CVE-2025-55224, CVE-2025-54915, CVE-2025-54912, CVE-2025-54910, CVE-2025-54901, CVE-2025-54900, CVE-2025-54116, CVE-2025-54115, CVE-2025-54113, CVE-2025-54112, CVE-2025-54105, CVE-2025-54104, CVE-2025-54103, CVE-2025-54094, CVE-2025-54093, CVE-2025-54091, CVE-2025-53810, CVE-2025-53809, CVE-2025-53807, CVE-2025-53806, CVE-2025-53805, CVE-2025-53802, CVE-2025-53801, CVE-2025-53800, CVE-2025-53799, CVE-2025-53796, CVE-2025-47997, CVE-2025-49692, CVE-2025-55317, CVE-2025-55316, CVE-2025-55243, CVE-2025-55245, CVE-2025-55226, CVE-2025-55225, CVE-2025-55223, CVE-2025-54918, CVE-2025-54916, CVE-2025-54908, CVE-2025-54907, CVE-2025-54906, CVE-2025-54905, CVE-2025-54904, CVE-2025-54903, CVE-2025-54898, CVE-2025-54897, CVE-2025-54896, CVE-2025-54895, CVE-2025-54111, CVE-2025-54110, CVE-2025-54106, CVE-2025-54101, CVE-2025-54099, CVE-2025-54097, CVE-2025-54095, CVE-2025-53798, CVE-2025-53797, CVE-2025-49734, CVE-2025-9867, CVE-2025-9866, CVE-2025-9865, CVE-2025-9864, CVE-2025-53791, CVE-2025-55241, CVE-2025-55238, CVE-2025-54914, CVE-2025-55242, CVE-2025-55244)
Description	Microsoft has released monthly security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected system. Microsoft advises to apply security fixes at your earliest to protect systems from potential threats
Affected Products	Azure Bot Service Azure Connected Machine Agent Azure Networking Dynamics 365 FastTrack Implementation Microsoft AutoUpdate for Mac Microsoft Edge (Chromium-based) Windows Server 2012 Windows Server 2012 (Server Core installation) Windows Server 2012 R2 Windows Server 2012 R2 (Server Core installation) Windows Server 2016 Windows Server 2016 (Server Core installation) Windows Server 2019 Windows Server 2019 (Server Core installation) Windows Server 2022 Windows Server 2022 (Server Core installation) Windows Server 2022, 23H2 Edition (Server Core installation) Windows Server 2025 Windows Server 2025 (Server Core installation) Xbox Gaming Services Microsoft Excel 2016 (32-bit edition) Microsoft Excel 2016 (64-bit edition) Microsoft HPC Pack 2019 Microsoft Office 2016 (32-bit edition) Microsoft Office 2016 (64-bit edition) Microsoft Office 2019 for 32-bit editions Microsoft Office 2019 for 64-bit editions Microsoft Office for Android Microsoft Office LTSC 2021 for 32-bit editions Microsoft Office LTSC 2021 for 64-bit editions Microsoft Office LTSC 2024 for 32-bit editions Microsoft Office LTSC 2024 for 64-bit editions Microsoft Office LTSC for Mac 2021 Microsoft Office LTSC for Mac 2024 Microsoft OfficePLUS Microsoft PowerPoint 2016 (32-bit edition) Microsoft PowerPoint 2016 (64-bit edition) Microsoft SharePoint Enterprise Server 2016 Microsoft SharePoint Server 2019 Microsoft SharePoint Server Subscription Edition Microsoft SQL Server 2017 for x64-based Systems (CU 31) Microsoft SQL Server 2017 for x64-based Systems (GDR) Microsoft SQL Server 2019 for x64-based Systems (CU 32) Microsoft SQL Server 2019 for x64-based Systems (GDR) Microsoft SQL Server 2022 for x64-based Systems (CU 20) Microsoft SQL Server 2022 for x64-based Systems (GDR) Microsoft Entra ID Microsoft Word 2016 (32-bit edition) Microsoft Word 2016 (64-bit edition) Office Online Server Microsoft 365 Apps for Enterprise for 32-bit Systems Microsoft 365 Apps for Enterprise for 64-bit Systems Windows 10 for 32-bit Systems Windows 10 for x64-based Systems Windows 10 Version 1607 for 32-bit Systems Windows 10 Version 1607 for x64-based Systems Windows 10 Version 1809 for 32-bit Systems Windows 10 Version 1809 for x64-based Systems Windows 10 Version 21H2 for 32-bit Systems Windows 10 Version 21H2 for ARM64-based Systems Windows 10 Version 21H2 for x64-based Systems Windows 10 Version 22H2 for 32-bit Systems Windows 10 Version 22H2 for ARM64-based Systems Windows 10 Version 22H2 for x64-based Systems Windows 11 Version 22H2 for ARM64-based Systems Windows 11 Version 22H2 for x64-based Systems Windows 11 Version 23H2 for ARM64-based Systems Windows 11 Version 23H2 for x64-based Systems Windows 11 Version 24H2 for ARM64-based Systems Windows 11 Version 24H2 for x64-based Systems Windows Server 2008 for 32-bit Systems Service Pack 2 Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) Windows Server 2008 for x64-based Systems Service Pack 2 Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) Windows Server 2008 R2 for x64-based Systems Service Pack 1 Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) Microsoft SQL Server 2016 for x64-based Systems Service Pack 3 (GDR) Microsoft SQL Server 2016 for x64-based Systems Service Pack 3 Azure Connect Feature Pack
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://msrc.microsoft.com/update-guide/vulnerability

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
Description	SUSE has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected system. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	OpenSUSE Leap 15.3 SUSE Linux Enterprise High Performance Computing 15 SP3 SUSE Linux Enterprise Live Patching 15-SP3, 15-SP6, 15-SP7 SUSE Linux Enterprise Micro 5.1, 5.2 SUSE Linux Enterprise Real Time 15 SP6, 15 SP7 SUSE Linux Enterprise Server 15 SP3, 15 SP6, 15 SP7 SUSE Linux Enterprise Server for SAP Applications 15 SP3, 15 SP6, 15 SP7
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2025/suse-su-202503097-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202503100-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202503105-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202503106-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202503104-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202503108-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202503109-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202503110-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202503111-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202503123-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202503124-1/

Affected Product	**Citrix**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-27466, CVE-2025-58142, CVE-2025-58143, CVE-2025-58146)
Description	Citrix has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected system. Citrix advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Citrix XenServer 8.4.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX695195&articleURL=XenServer_Security_Update_for_CVE_2025_27466_CVE_2025_58142_CVE_2025_58143_and_CVE_2025_58146

Affected Product	**F5**
Severity	**High**
Affected Vulnerability	RADIUS Protocol Authentication Vulnerability (CVE-2024-3596)
Description	F5 has released a security update addressing a RADIUS protocol authentication vulnerability that exist in their products **CVE-2024-3596** - This vulnerability allows attackers to forge authentication responses when the Message-Authenticator attribute is not enforced. Resulting in unauthorized access by modifying an Access-Reject response to an Access-Accept response, thereby compromising the authentication process. F5 advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	BIG-IP (all modules) Versions - 17.1.0 - 17.1.1, 16.1.0 - 16.1.5, 15.1.0 - 15.1.10
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://my.f5.com/manage/s/article/K000141008

Affected Product	**IBM**
Severity	**High**
Affected Vulnerability	Authorization Bypass Vulnerability (CVE-2025-3319)
Description	IBM has released a security update addressing an authorization bypass vulnerability that exists in their products. **CVE-2025-3319** - IBM Spectrum Protect Server could allow attacker to bypass authentication due to improper session authentication which can result in access to unauthorized resources. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Storage Protect Server Versions - 8.1.0.000 - 8.1.26.000
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7236999

Affected Product	**Ivanti**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-9712, CVE-2025-9872, CVE-2025-8712, CVE-2025-8711, CVE-2025-55145, CVE-2025-55146, CVE-2025-55147, CVE-2025-55148, CVE-2025-55139, CVE-2025-55141, CVE-2025-55142, CVE-2025-55143, CVE-2025-55144)
Description	Ivanti has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause remote code execution, privilege escalation and denial of service. Ivanti advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	ZTA Gateways Versions - 22.8R2.2 Ivanti Policy Secure Versions - 22.7R1.4 and prior Ivanti Connect Secure Versions - 22.7R2.8 and prior Ivanti Endpoint Manager Versions - 2024 SU3 and prior Neurons for Secure Access Versions - 22.8R1.3 and prior Ivanti Endpoint Manager Versions - 2022 SU8 Security Update 1 and prior
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://forums.ivanti.com/s/article/Security-Advisory-September-2025-for-Ivanti-EPM-2024-SU3-and-EPM-2022-SU8?language=en_US • https://forums.ivanti.com/s/article/September-Security-Advisory-Ivanti-Connect-Secure-Policy-Secure-ZTA-Gateways-and-Neurons-for-Secure-Access-Multiple-CVEs?language=en_US

Affected Product	**Fortinet**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-45325, CVE-2025-53609)
Description	Fortinet has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2024-45325** - An improper neutralization of special elements used in an OS command ('OS Command Injection') vulnerability in FortiDDoS-F CLI may allow a privileged attacker to execute unauthorized code or commands via crafted CLI requests. **CVE-2025-53609** - A Relative Path Traversal vulnerability in FortiWeb may allow an authenticated attacker to perform an arbitrary file read on the underlying system via crafted requests. Fortinet advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	FortiDDoS-F 6.6 - 6.6 all versions FortiDDoS-F 6.5 - 6.5 all versions FortiDDoS-F 6.4 - 6.4 all versions FortiDDoS-F 6.3 - 6.3 all versions FortiDDoS-F 6.2 - 6.2 all versions FortiDDoS-F 6.1 - 6.1 all versions FortiWeb 7.6 - 7.6.0 through 7.6.4 FortiWeb 7.4 - 7.4.0 through 7.4.8 FortiWeb 7.2 - 7.2.0 through 7.2.11 FortiWeb 7.0 - 7.0.2 through 7.0.11 FortiDDoS-F 7.0 - 7.0.0 through 7.0.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.fortiguard.com/psirt/FG-IR-24-344 • https://www.fortiguard.com/psirt/FG-IR-25-512

Disclaimer

The information provided are gathered from official service provider's websites and portals. FinCSIRT strongly recommends members to apply security fixes as per the given guidelines, following the organization's patch and change management procedures to protect systems from potential threats.