Advisory Alert

Alert Number: AAA20251015 **Date:** October 15, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Veeam	**Critical**	Multiple Vulnerabilities
Dell	**Critical**	Multiple Vulnerabilities
Microsoft	**Critical**	Multiple Vulnerabilities
Veeam	**High**	Security Update
Red Hat	**High**, Medium	Multiple Vulnerabilities
Ivanti	**High**, Medium	Multiple Vulnerabilities
IBM	**High**, Medium	Multiple Vulnerabilities
Fortinet	**High**, Medium, Low	Multiple Vulnerabilities
F5	Low	DNS Resource Exhaustion Vulnerability

Description

Affected Product	**Veeam**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-48983, CVE-2025-48984)
Description	Veeam has released security updates addressing multiple vulnerabilities that exist in Veeam Backup & Replication. **CVE-2025-48983** - A vulnerability in the Mount service of Veeam Backup & Replication, which allows for remote code execution (RCE) on the Backup infrastructure hosts by an authenticated domain user. **CVE-2025-48984** - A vulnerability allowing remote code execution (RCE) on the Backup Server by an authenticated domain user. Veeam advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Veeam Backup & Replication 12.3.2.3617 and all earlier version 12 builds
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.veeam.com/kb4771

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-6780, CVE-2024-480, CVE-2024-25571, CVE-2024-28956, CVE-2024-2961, CVE-2024-21859, CVE-2024-28047, CVE-2024-31068, CVE-2024-31155, CVE-2024-36293, CVE-2024-37020, CVE-2024-38796, CVE-2024-39279, CVE-2024-45332, CVE-2024-45490, CVE-2024-45491, CVE-2024-45492, CVE-2024-50602, CVE-2024-52533, CVE-2025-20044, CVE-2025-20053, CVE-2025-20109, CVE-2025-20613, CVE-2025-21090, CVE-2025-21096, CVE-2025-22853, CVE-2025-24305, CVE-2025-26466)
Description	Dell has released security updates addressing multiple vulnerabilities that exist in Dell PowerScale OneFS. These vulnerabilities could be exploited by malicious users to compromise the affected system. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	PowerScale Node Firmware Package Versions prior to 13.1.3 of: PowerScale F200, PowerScale F900, PowerScale P100, PowerScale F710 PowerScale F600, PowerScale B100, PowerScale F210, PowerScale F910
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000363693/dsa-2025-166-security-update-for-dell-powerscale-onefs-multiple-third-party-component-vulnerabilities

Affected Product	**Microsoft**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities
Description	Microsoft has released monthly security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Elevation of Privilege, Denial of Service, Information Disclosure, Remote Code Execution, Security Feature Bypass, Spoofing and Tampering attempts. Microsoft advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	• Windows 11 Version 25H2 for ARM64-based Systems • Windows 11 Version 25H2 for x64-based Systems • Windows Server 2016 (Server Core installation) • Windows Server 2016 • Windows 10 Version 1607 for x64-based Systems • Windows 10 Version 1607 for 32-bit Systems • Windows 10 for x64-based Systems • Windows 11 Version 23H2 for x64-based Systems • Windows 11 Version 23H2 for ARM64-based Systems • Windows Server 2025 (Server Core installation) • 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 x64-based Systems • Windows 11 Version 22H2 for ARM64-based Systems • Windows 10 Version 21H2 for x64-based Systems • Windows Server 2008 for x64-based Systems Service Pack 2 • Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) • Windows Server 2008 for 32-bit Systems Service Pack 2 • Windows 10 for 32-bit Systems • Windows Server 2025 • Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) • Windows Server 2008 R2 for x64-based Systems Service Pack 1 • Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) • Windows Server 2012, 2019 • Windows 10 Version 1809 for x64-based Systems • Windows 10 Version 1809 for 32-bit Systems • Windows 11 Version 24H2 for x64-based Systems • Windows 11 Version 24H2 for ARM64-based Systems • Windows Server 2022, 23H2 Edition (Server Core installation) • Windows Server 2019 (Server Core installation) • Microsoft PowerPoint 2016 (64-bit edition) • Microsoft PowerPoint 2016 (32-bit edition) • Microsoft Office LTSC 2024 for 32 and 64-bit editions • Microsoft Office LTSC 2021 for 32 and 64-bit editions • Microsoft 365 Apps for Enterprise for 32 and 64-bit Systems • Microsoft Office 2019 for 64-bit editions • Microsoft Office 2019 for 32-bit editions • Microsoft Access 2016 (64-bit edition) • Microsoft Office LTSC for Mac 2024 • Windows 10 Version 21H2 for ARM64-based Systems • Windows 10 Version 21H2 for 32-bit Systems • Microsoft Office LTSC for Mac 2021 • Microsoft SharePoint Server 2019 • Microsoft SharePoint Enterprise Server 2016 • Microsoft Word 2016 (64-bit edition) • Microsoft Word 2016 (32-bit edition) • Microsoft Configuration Manager 2403, 2503, 2409 • Windows Server 2022 (Server Core installation) • Windows Server 2012 R2 (Server Core installation) • Windows Server 2012 R2 • Windows Server 2012 (Server Core installation) • Microsoft Exchange Server 2019 Cumulative Update 14, 15 • Microsoft Exchange Server 2016 Cumulative Update 23 • Microsoft Exchange Server Subscription Edition RTM • Windows Server 2022 • Microsoft Access 2016 (32-bit edition) • Microsoft Excel 2016 (32 and 64-bit editions) • Microsoft Excel 2016 (32-bit edition) • Office Online Server • Microsoft Office for Android • Microsoft .NET Framework 3.5 • Microsoft .NET Framework 2.0, 3.0 Service Pack 2 • microsoft/playwright • Microsoft Defender for Endpoint for Linux • Azure Monitor Agent • Arc Enabled Servers - Azure Connected Machine Agent • Remote Desktop client for Windows Desktop • Windows App Client for Windows Desktop • Microsoft .NET Framework 3.5, 4.6.2, 4.6.2, 4.7, 4.8 • Microsoft Visual Studio 2022 version 17.14, 17.10, 17.12 • .NET 8.0 installed on Windows, Mac OS, Linux • .NET 9.0 installed on Windows, Mac OS, Linux • Microsoft Visual Studio 2019 version 16.11 (includes 16.0 - 16.10) • Microsoft Visual Studio 2017 version 15.9 (includes 15.0 - 15.8) • PowerShell 7.5, 7.4 • Azure Compute Gallery • Xbox Gaming Services • Microsoft JDBC Driver 12.10, 13.2, 12.6, 11.2, 10.2, 12.8, 12.2, 12.4 for SQL Server • Microsoft SharePoint Server Subscription Edition • ASP.NET Core 2.3, 9.0, 8.0 • Azure Confidential Compute VM SKU ECasv6/ECadsv6 • Azure Confidential Compute VM SKU DCasv6/DCadsv6 • Azure Confidential Compute VM SKU DCasv5/DCadsv5 • Azure Confidential Compute VM SKU ECasv5/ECadsv5 • Microsoft Edge (Chromium-based) • Microsoft 365 Copilot's Business Chat • Azure Managed Redis • Azure Cache for Redis Enterprise • Microsoft 365 Word Copilot • Azure Monitor • Azure PlayFab • Microsoft Entra ID • Microsoft Mesh for Meta Quest • Microsoft Mesh PC Applications
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://msrc.microsoft.com/update-guide/releaseNote/2025-Oct

Affected Product	**Veeam**
Severity	**High**
Affected Vulnerability	Security Update (CVE-2025-48982)
Description	Veeam has released security updates addressing a vulnerability that exist in Veeam Agent for Microsoft Windows. **CVE-2025-48982** - This vulnerability in Veeam Agent for Microsoft Windows allows for Local Privilege Escalation if a system administrator is tricked into restoring a malicious file. Veeam advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Veeam Agent for Microsoft Windows 6.3.2.1205 and all earlier version 6 builds
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.veeam.com/kb4771

Affected Product	**Red Hat**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-49969, CVE-2022-49985, CVE-2022-50087, CVE-2022-50229, CVE-2023-53125, CVE-2023-53186, CVE-2025-22097, CVE-2025-37914, CVE-2025-38211, CVE-2025-38392, CVE-2025-38449, CVE-2025-38461, CVE-2025-38498, CVE-2025-38550, CVE-2025-38566)
Description	Red Hat 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. Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 9.4 aarch64 Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 9.4 s390x Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 9.4 ppc64le Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 9.4 x86_64 Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.4 aarch64 Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.4 aarch64 Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.4 s390x Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.4 s390x Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.4 ppc64le Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.4 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support Extension 8.6 x86_64 Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.6 x86_64 Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.2 x86_64 Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.4 x86_64 Red Hat Enterprise Linux Server - AUS 8.6 x86_64 Red Hat Enterprise Linux Server - AUS 9.2 x86_64 Red Hat Enterprise Linux Server - AUS 9.4 x86_64 Red Hat Enterprise Linux Server - TUS 8.6 x86_64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.6 ppc64le Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.2 ppc64le Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.4 ppc64le
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2025:17958 • https://access.redhat.com/errata/RHSA-2025:17896 • https://access.redhat.com/errata/RHSA-2025:18043

Affected Product	**Ivanti**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-10242, CVE-2025-10243, CVE-2025-10985, CVE-2025-10986)
Description	Ivanti has released security updates addressing multiple vulnerabilities that exist in Ivanti Endpoint Manager Mobile. These vulnerabilities could be exploited by malicious users to cause Remote Code Execution, Path traversal and OS Command Injection. Ivanti advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ivanti Endpoint Manager Mobile (EPMM) versions: • 12.6.0.1 • 12.5.0.2 • 12.4.0.3 and prior
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://forums.ivanti.com/s/article/Security-Advisory-Endpoint-Manager-Mobile-EPMM-10-2025-Multiple-CVEs?language=en_US

Affected Product	**IBM**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-48976, CVE-2025-27553, CVE-2025-30474, CVE-2025-25193)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Denial of Service, Path Traversal, and Exposure of Sensitive Information. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Storage Scale versions 5.1.9.0 - 5.1.9.11 and 5.2.0.0 - 5.2.3.2 WebSphere Extreme Scale versions 8.6.1.0 - 8.6.1.6
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7247935 • https://www.ibm.com/support/pages/node/7247893

Affected Product	**Fortinet**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-46718, CVE-2024-26008, CVE-2024-33507, CVE-2024-47569, CVE-2024-50571, CVE-2025-22258, CVE-2025-25252, CVE-2025-25253, CVE-2025-25255, CVE-2025-31365, CVE-2025-31366, CVE-2025-31514, CVE-2025-46774, CVE-2025-49201, CVE-2025-53845, CVE-2025-54822, CVE-2025-54973, CVE-2025-57716, CVE-2025-57740, CVE-2025-57741, CVE-2025-58324, CVE-2025-58325, CVE-2025-58903, CVE-2025-59921)
Description	Fortinet has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Denial of Service, Information Disclosure, Execute Unauthorized Code or Commands, Escalation of privilege. Fortinet advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.fortiguard.com/psirt

Affected Product	**F5**
Severity	**Low**
Affected Vulnerability	DNS Resource Exhaustion Vulnerability (CVE-2024-11187)
Description	F5 has released security updates addressing a DNS Resource Exhaustion Vulnerability that exists in BIG-IP modules. **CVE-2024-11187** - It is possible to construct a zone such that some queries to it will generate responses containing numerous records in the Additional section. An attacker sending many such queries can cause either the authoritative server itself or an independent resolver to use disproportionate resources processing the queries. Zones will usually need to have been deliberately crafted to attack this exposure. F5 advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	BIG-IP (all modules) versions: • 17.5.0 - 17.5.1 • 17.1.0 - 17.1.2 • 16.1.0 - 16.1.6 • 15.1.0 - 15.1.10
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://my.f5.com/manage/s/article/K000150814

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.