Advisory Alert

Alert Number: AAA20250709 **Date:** July 9, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Microsoft	**Critical**	Multiple Vulnerabilities
IBM	**Critical**	Multiple Vulnerabilities
SAP	**Critical**	Multiple Vulnerabilities
Fortinet	**Critical**	Unauthenticated SQL injection Vulnerability
Lenovo	**High**	Multiple BIOS Vulnerabilities
Red Hat	**High**	Multiple Vulnerabilities
SUSE	**High**	Multiple Vulnerabilities
Dell	**High**, Medium	Multiple Vulnerabilities
Ivanti	**High**, Medium	Multiple Vulnerabilities
Ubuntu	**High**, Medium	Multiple Vulnerabilities
IBM	**High**, Medium, Low	Multiple Vulnerabilities
SAP	**High**, Medium, Low	Multiple Vulnerabilities
AMD	Medium	Multiple Transient Execution Vulnerabilities
Fortinet	Medium, Low	Multiple Vulnerabilities

Description

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 compromise the affected system. Microsoft advises to apply security fixes at your earliest to protect systems from potential threats.	
Affected Products	Microsoft Edge (Chromium-based) Windows Storage Office Developer Platform Microsoft Graphics Component Windows SmartScreen Visual Studio Microsoft PC Manager Microsoft Teams Windows KDC Proxy Service (KPSSVC) Windows Win32K - ICOMP Microsoft Windows QoS scheduler Windows Win32K - GRFX Windows Notification Windows StateRepository API Windows Print Spooler Components Windows Fast FAT Driver SQL Server Windows Netlogon Visual Studio Code - Python extension Microsoft Office Excel Microsoft Office SharePoint Microsoft Office PowerPoint Microsoft Office Word Microsoft Office Microsoft Brokering File System Windows Media Virtual Hard Disk (VHDX) Microsoft Input Method Editor (IME) Windows TCP/IP Storage Port Driver Windows Performance Recorder Windows Shell Windows NTFS AMD L1 Data Queue AMD Store Queue Visual Studio Code .NET and Visual Studio Service Fabric Servicing Stack Updates	Kernel Streaming WOW Thunk Service Driver Windows Kernel Workspace Broker Windows User-Mode Driver Framework Host Windows Ancillary Function Driver for WinSock Windows Event Tracing Windows TDX.sys Windows Cryptographic Services Role: Windows Hyper-V Windows Universal Plug and Play (UPnP) Device Host Windows AppX Deployment Service Windows BitLocker Remote Desktop Client HID class driver Windows SSDP Service Windows Remote Desktop Licensing Service Windows Virtualization-Based Security (VBS) Enclave Windows Secure Kernel Mode Microsoft MPEG-2 Video Extension Windows SMB Windows Update Service Windows MBT Transport driver Azure Monitor Agent Windows Cred SSProvider Protocol Universal Print Management Service Windows GDI Windows Storage VSP Driver Windows SPNEGO Extended Negotiation Windows Imaging Component Windows Kerberos Microsoft Configuration Manager Microsoft Defender for Endpoint Windows Routing and Remote Access Service (RRAS) Windows Connected Devices Platform Service Dynamics 365 FastTrack Implementation Assets Capability Access Management Service (camsvc) Microsoft Windows Search Component	
Officially Acknowledged by the Vendor	Yes	
Patch/ Workaround Released	Yes	
Reference	https://msrc.microsoft.com/update-guide/vulnerability	

Affected Product	**IBM**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2016-1000027, CVE-2021-32760)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in IBM DB2 Data Management Console. **CVE-2016-1000027** - Pivotal Spring Framework through 5.3.16 suffers from a potential remote code execution (RCE) issue if used for Java deserialization of untrusted data. Depending on how the library is implemented within a product, this issue may or not occur, and authentication may be required. NOTE: the vendor's position is that untrusted data is not an intended use case. The product's behavior will not be changed because some users rely on deserialization of trusted data. **CVE-2021-32760** - containerd is a container runtime. A bug was found in containerd versions prior to 1.4.8 and 1.5.4 where pulling and extracting a specially-crafted container image can result in Unix file permission changes for existing files in the host's filesystem. Changes to file permissions can deny access to the expected owner of the file, widen access to others, or set extended bits like setuid, setgid, and sticky. This bug does not directly allow files to be read, modified, or executed without an additional cooperating process. This bug has been fixed in containerd 1.5.4 and 1.4.8. As a workaround, ensure that users only pull images from trusted sources. Linux security modules (LSMs) like SELinux and AppArmor can limit the files potentially affected by this bug through policies and profiles that prevent containerd from interacting with specific files. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM DB2 Data Management Console versions 3.1.11 - 3.1.13 IBM DB2 Data Management Console on CPD 4.7.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7239178

Affected Product	**SAP**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-30012, CVE-2025-42967, CVE-2025-42980, CVE-2025-42964, CVE-2025-42966, CVE-2025-42963)
Description	SAP has released monthly security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Code Injection, Insecure Deserialization and low impact on confidentiality and integrity. SAP advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	• SAP Supplier Relationship Management (Live Auction Cockpit) Version – SRM_SERVER 7.14 • SAP S/4HANA and SAP SCM (Characteristic Propagation) Versions – SCMAPO 713, 714, S4CORE 102, 103, 104, S4COREOP 105, 106, 107, 108, SCM 700, 701, 702, 712 • SAP NetWeaver Enterprise Portal Federated Portal Network Version – EP-RUNTIME 7.50 • SAP NetWeaver Enterprise Portal Administration Version – EP-RUNTIME 7.50 • SAP NetWeaver (XML Data Archiving Service) Versions – J2EE-APPS 7.50
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.sap.com/en/my-support/knowledge-base/security-notes-news/july-2025.html

Affected Product	**Fortinet**
Severity	**Critical**
Affected Vulnerability	Unauthenticated SQL injection Vulnerability (CVE-2025-25257)
Description	Fortinet has released security updates addressing an Unauthenticated SQL injection Vulnerability that exists in FortiWeb. **CVE-2025-25257** - An improper neutralization of special elements used in an SQL command ('SQL Injection') vulnerability in FortiWeb may allow an unauthenticated attacker to execute unauthorized SQL code or commands via crafted HTTP or HTTPs requests. Fortinet advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	FortiWeb 7.6 versions 7.6.0 through 7.6.3 FortiWeb 7.4 versions 7.4.0 through 7.4.7 FortiWeb 7.2 versions 7.2.0 through 7.2.10 FortiWeb 7.0 versions 7.0.0 through 7.0.10
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.fortiguard.com/psirt/FG-IR-25-151

Affected Product	**Lenovo**
Severity	**High**
Affected Vulnerability	Multiple BIOS Vulnerabilities (CVE-2024-36348, CVE-2024-36349, CVE-2024-36350, CVE-2024-36357, CVE-2024-48869, CVE-2025-20004, CVE-2025-20100)
Description	Lenovo has released security updates addressing multiple BIOS vulnerabilities that exist in a third party product which affects Lenovo products. These vulnerabilities could be exploited by malicious users to cause Information Disclosure and Privilege Escalation. Lenovo 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://support.lenovo.com/us/en/product_security/LEN-200962

Affected Product	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-27611, CVE-2025-2901, CVE-2025-2251, CVE-2025-23184, CVE-2025-48734)
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 affected systems. Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	JBoss Enterprise Application Platform 8.0 for RHEL 8 x86_64 JBoss Enterprise Application Platform Text-Only Advisories x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2025:10459 • https://access.redhat.com/errata/RHSA-2025:10452

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 15.6 Public Cloud Module 15-SP6, 15-SP7 SUSE Linux Enterprise Server 15 SP6. 15 SP7 SUSE Linux Enterprise Server for SAP Applications 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-202502254-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202502249-1/

Affected Product	**Dell**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-21446, CVE-2025-21449, CVE-2025-21454, CVE-2025-36599)
Description	Dell has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise affected systems. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	PowerFlex Manager - 4.6.2 and prior versions Inspiron 14 5441 - Versions prior to 1.0.4237.8400 Inspiron 14 7441 - Versions prior to 1.0.4237.8400 Latitude 5455 - Versions prior to 1.0.4237.8400 Latitude 7455 - Versions prior to 1.0.4237.8400 XPS 13 9345 - Versions prior to 1.0.4237.8400
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000294901/dsa-2025-128 • https://www.dell.com/support/kbdoc/en-us/000342158/dsa-2025-279-security-update-for-dell-powerflex-manager-platform-pfmp-proprietary-code-vulnerability

Affected Product	**Ivanti**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-6770, CVE-2025-6771, CVE-2025-6995, CVE-2025-6996, CVE-2025-7037, CVE-2025-5450, CVE-2025-5451, CVE-2025-5463, CVE-2025-5464, CVE-2025-0293, CVE-2025-0292)
Description	Ivanti has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Information Disclosure, Denial of Service, Remote Code Execution, data modification. Ivanti advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ivanti Endpoint Manager Mobile versions : 12.5.0.1 and prior 12.4.0.2 and prior 12.3.0.2 and prior Ivanti Endpoint Manager : 2022 SU8 and prior 2024 SU2 and prior Ivanti Connect Secure (ICS) : 22.7R2.7 and prior 22.7R1.4 and prior
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Endpoint-Manager-Mobile-EPMM-CVE-2025-6770-CVE-2025-6771?language=en_US • https://forums.ivanti.com/s/article/Security-Advisory-July-2025-for-Ivanti-EPM-2024-SU2-and-EPM-2022-SU8?language=en_US • https://forums.ivanti.com/s/article/July-Security-Advisory-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Multiple-CVEs?language=en_US

Affected Product	**Ubuntu**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-38000, CVE-2025-37932, CVE-2025-37798, CVE-2024-56662, CVE-2024-53197, CVE-2024-50116, CVE-2024-49958, CVE-2024-46787, CVE-2024-41070, CVE-2022-49179, CVE-2022-49176, CVE-2021-47379)
Description	Ubuntu 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. Ubuntu advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ubuntu 18.04 Ubuntu 16.04 Ubuntu 14.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-7627-1

Affected Product	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-41103, CVE-2022-23471, CVE-2022-23648, CVE-2022-31030, CVE-2022-32149, CVE-2023-25153, CVE-2023-25173, CVE-2021-35515, CVE-2021-35516, CVE-2021-35517, CVE-2021-36090, CVE-2024-25710, CVE-2020-13956)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in IBM DB2 Data Management Console and QRadar SIEM. These vulnerabilities could be exploited by malicious users to cause Privilege Escalation, Denial of Service, request smuggling, command execution. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM DB2 Data Management Console versions 3.1.11 - 3.1.13 IBM DB2 Data Management Console on CPD v4.7.1 IBM QRadar SIEM versions 7.5 - 7.5.0 UP12 IF02
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7239178 • https://www.ibm.com/support/pages/node/7239009

Affected Product	**SAP**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-42959, CVE-2025-42953, CVE-2024-53677, CVE-2025-42952, CVE-2025-42977, CVE-2025-43001, CVE-2025-42992, CVE-2025-42993, CVE-2025-42997, CVE-2025-42981, CVE-2025-42956, CVE-2025-42969, CVE-2025-42962, CVE-2025-42985, CVE-2025-42970, CVE-2025-42979, CVE-2025-42973, CVE-2025-42968, CVE-2025-42961, CVE-2025-42960, CVE-2025-42986, CVE-2025-42974, CVE-2025-31326, CVE-2025-42965, CVE-2025-42971, CVE-2025-42978, CVE-2025-42954)
Description	SAP has released monthly security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Directory Traversal, Information Disclosure, Cross-Site Scripting, Server Side Request Forgery, Denial of service. SAP 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://support.sap.com/en/my-support/knowledge-base/security-notes-news/july-2025.html

Affected Product	**AMD**
Severity	**Medium**
Affected Vulnerability	Multiple Transient Execution Vulnerabilities (CVE-2024-36350, CVE-2024-36357, CVE-2024-36348, CVE-2024-36349)
Description	AMD has released security updates addressing Multiple Transient Execution Vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Sensitive Information Disclosure. AMD 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.amd.com/en/resources/product-security/bulletin/amd-sb-7029.html

Affected Product	**Fortinet**
Severity	**Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-32124, CVE-2024-55599, CVE-2025-24477, CVE-2024-52965, CVE-2025-24474, CVE-2024-27779)
Description	Fortinet has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Execute Unauthorized Code or Commands, Escalation of Privilege and Improper access control. 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/FG-IR-24-045 • https://www.fortiguard.com/psirt/FG-IR-24-053 • https://www.fortiguard.com/psirt/FG-IR-25-026 • https://www.fortiguard.com/psirt/FG-IR-24-511 • https://www.fortiguard.com/psirt/FG-IR-24-437 • https://www.fortiguard.com/psirt/FG-IR-24-035

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.