Advisory Alert

Alert Number: AAA20250724 **Date:** July 24, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
SonicWall	**Critical**	Post-authentication Arbitrary File Upload vulnerability
IBM	**Critical**	Arbitrary Code Execution Vulnerability
Dell	**High**	Multiple Vulnerabilities
SonicWall	**High**	Multiple Vulnerabilities
IBM	**High**, **Medium**, **Low**	Multiple Vulnerabilities
Apache HTTP Server	**Medium**	Security Update
Drupal	**Medium**	Cross-site Scripting Vulnerability
HPE	**Medium**	Multiple Vulnerabilities
F5	**Low**	Multiple Vulnerabilities

Description

Affected Product	**SonicWall**
Severity	**Critical**
Affected Vulnerability	Post-authentication Arbitrary File Upload vulnerability (CVE-2025-40599)
Description	SonicWall has released security updates addressing a Post-authentication Arbitrary File Upload vulnerability that exists in SonicWall SMA 100 series web management interface. **CVE-2025-40599** - An authenticated arbitrary file upload vulnerability exists in the SMA 100 series web management interface. A remote attacker with administrative privileges can exploit this flaw to upload arbitrary files to the system, potentially leading to remote code execution. SonicWall advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	SMA 100 Series (SMA 210, 410, 500v) 10.2.1.15-81sv and earlier versions.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2025-0014

Affected Product	**IBM**
Severity	**Critical**
Affected Vulnerability	Arbitrary Code Execution Vulnerability (CVE-2025-30065)
Description	IBM has released security updates addressing an Arbitrary Code Execution Vulnerability that exists in Apache Parquet which affects IBM Db2 Server. **CVE-2025-30065** - Schema parsing in the parquet-avro module of Apache Parquet 1.15.0 and previous versions allows bad actors to execute arbitrary code. The affected libraries are present as part of Db2 and could be accidentally used by some method outside of Db2 or a future change to the FEDERATION setting. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Db2 Server versions 11.1.0 - 11.1.4.7, 11.5.0 - 11.5.9 and 12.1.0 - 12.1.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7235042

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-3596, CVE-2021-26720, CVE-2020-7105, CVE-2024-38428, CVE-2025-1795, CVE-2024-2398, CVE-2024-8096, CVE-2024-50602, CVE-2025-32414, CVE-2025-32415, CVE-2025-21605, CVE-2023-4738, CVE-2023-5344, CVE-2024-22667, CVE-2024-43802, CVE-2024-47814, CVE-2025-46836, CVE-2025-3576, CVE-2025-0395, CVE-2025-4802, CVE-2025-5222)
Description	Dell has released security updates addressing multiple vulnerabilities that exist in Dell Networking OS10. 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	Dell Networking OS10 versions prior to 10.5.4.16
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000348734/dsa-2025-285-security-update-for-dell-networking-os10-vulnerabilities

Affected Product	**SonicWall**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-40596, CVE-2025-40597, CVE-2025-40598)
Description	SonicWall has released security updates addressing multiple vulnerabilities that exist in SonicWall SMA 100 series web management interface. **CVE-2025-40596** - A Stack-based buffer overflow vulnerability in the SMA100 series web interface allows remote, unauthenticated attacker to cause Denial of Service (DoS) or potentially results in code execution. **CVE-2025-40597** - A Heap-based buffer overflow vulnerability in the SMA100 series web interface allows remote, unauthenticated attacker to cause Denial of Service (DoS) or potentially results in code execution. **CVE-2025-40598** - A Reflected cross-site scripting (XSS) vulnerability exists in the SMA100 series web interface, allowing a remote unauthenticated attacker to potentially execute arbitrary JavaScript code. SonicWall advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	SMA 100 Series (SMA 210, 410, 500v) 10.2.1.15-81sv and earlier versions.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2025-0012

Affected Product	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-7254, CVE-2022-3510, CVE-2022-3509, CVE-2022-3171, CVE-2025-2518, CVE-2024-23454, CVE-2024-49350, CVE-2024-52903, CVE-2025-0915, CVE-2025-1000, CVE-2025-1493, CVE-2025-1992)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in IBM Db2 Server. These vulnerabilities could be exploited by malicious users to cause Denial of Service and Sensitive Information Disclosure. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Db2 Server versions 11.1.0 - 11.1.4.7, 11.5.0 - 11.5.9 and 12.1.0 - 12.1.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7235067 • https://www.ibm.com/support/pages/node/7234906 • https://www.ibm.com/support/pages/node/7235072 • https://www.ibm.com/support/pages/node/7235070 • https://www.ibm.com/support/pages/node/7235069 • https://www.ibm.com/support/pages/node/7232336 • https://www.ibm.com/support/pages/node/7232529 • https://www.ibm.com/support/pages/node/7232528 • https://www.ibm.com/support/pages/node/7232518 • https://www.ibm.com/support/pages/node/7232515

Affected Product	**Apache HTTP Server**
Severity	**Medium**
Affected Vulnerability	Security Update (CVE-2025-54090)
Description	Apache has released security updates addressing a vulnerability that exists in Apache HTTP Server. **CVE-2025-54090** - A bug in Apache HTTP Server 2.4.64 results in all "RewriteCond expr ..." tests evaluating as "true". Apache advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Apache HTTP Server 2.4.64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://httpd.apache.org/security/vulnerabilities_24.html

Affected Product	**Drupal**
Severity	**Medium**
Affected Vulnerability	Cross-site Scripting vulnerability (CVE-2025-8092)
Description	Drupal has released security updates addressing a Cross-site Scripting vulnerability that exists in COOKiES Consent Management module. **CVE-2025-8092** - The module doesn't sufficiently check whether to convert "data-src" attributes to "src" when their value might contain malicious content under the scenario, that module specific classes are set on the HTML element. Drupal advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	COOKiES Consent Management versions prior to 1.2.16
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.drupal.org/sa-contrib-2025-092

Affected Product	**HPE**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-26465, CVE-2025-32728)
Description	HPE has released security updates addressing multiple vulnerabilities that exist in HP-UX. **CVE-2025-26465** - A vulnerability was found in OpenSSH when the VerifyHostKeyDNS option is enabled. A machine-in-the-middle attack can be performed by a malicious machine impersonating a legit server. This issue occurs due to how OpenSSH mishandles error codes in specific conditions when verifying the host key. For an attack to be considered successful, the attacker needs to manage to exhaust the client's memory resource first, turning the attack complexity high. **CVE-2025-32728** - In sshd in OpenSSH before 10.0, the DisableForwarding directive does not adhere to the documentation stating that it disables X11 and agent forwarding. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	HP-UX 11i Secure Shell Software versions prior to A.09.30.010
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbux04903en_us&docLocale=en_US

Affected Product	**F5**
Severity	**Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-58251, CVE-2025-46394)
Description	F5 has released security updates addressing multiple vulnerabilities that exist in BIG-IP Next products. **CVE-2024-58251** - In netstat in BusyBox through 1.37.0, local users can launch of network application with an argv[0] containing an ANSI terminal escape sequence, leading to a denial of service (terminal locked up) when netstat is used by a victim. **CVE-2025-46394** - In tar in BusyBox through 1.37.0, a TAR archive can have filenames hidden from a listing through the use of terminal escape sequences. F5 advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	BIG-IP Next SPK versions 1.7.0 - 1.9.2 and 2.0.0 - 2.0.1 BIG-IP Next CNF versions 1.1.0 - 1.4.1 and 2.0.0 - 2.0.1 BIG-IP Next for Kubernetes version 2.0.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://my.f5.com/manage/s/article/K000152678 • https://my.f5.com/manage/s/article/K000152680

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.