Advisory Alert

Alert Number: AAA20260619 **Date:** June 19, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Vendor	Severity	Vulnerability
F5	**High**	Configuration Injection Vulnerability
SUSE	**High**	Multiple Vulnerabilities
IBM	**High**, **Medium**	Improper Validation Vulnerability
NodeJS	**High**, **Medium**, **Low**	Multiple Vulnerabilities
cPanel	**High**, **Medium**, **Low**	Multiple Vulnerabilities

Description

Vendor	**F5**
Severity	**High**
Affected Vulnerability	Configuration Injection Vulnerability (CVE-2026-50107)
Description	F5 has released a security update addressing a vulnerability that exists in their product. **CVE-2026-50107:** When NGINX Plus or NGINX Open Source is configured as the data plane for NGINX Gateway Fabric, an injection vulnerability exists in the NGINX configuration generator component of NGINX Gateway Fabric. User-supplied string values from the NginxProxy Custom Resource Definition (CRD) access log format setting are rendered directly into NGINX configuration templates without sanitization or escaping. An authenticated attacker with permission to create or modify these CRDs may craft values that inject arbitrary NGINX configuration directives. F5 advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	NGINX Gateway Fabric - Version 2.3.0 - 2.6.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://my.f5.com/manage/s/article/K000161785

Vendor	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
Description	SUSE has released a security update addressing multiple vulnerabilities that exist in the kernel of their products. These vulnerabilities could be exploited by malicious users to compromise the affected systems. SUSE advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	SUSE Linux Enterprise High Performance Computing 12 SP5 SUSE Linux Enterprise Live Patching 12-SP5 SUSE Linux Enterprise Server 12 SP5 SUSE Linux Enterprise Server 12 SP5 LTSS SUSE Linux Enterprise Server 12 SP5 LTSS Extended Security SUSE Linux Enterprise Server for SAP Applications 12 SP5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2026/suse-su-20262450-1/

Vendor	**IBM**
Severity	**High**, **Medium**
Affected Vulnerability	Improper Validation Vulnerability (CVE-2026-1352)
Description	IBM has released a security update addressing a vulnerability that exists in their products. **CVE-2026-1352:** IBM Db2 11.5.0 through 11.5.9, and 12.1.0 through 12.1.4 for Linux, UNIX and Windows (includes Db2 Connect Server) could allow an authenticated user to cause a denial of service due to improper neutralization of special elements in data query logic. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Db2 Versions: • 11.5.0 - 11.5.9 • 12.1.0 - 12.1.4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7269433

Vendor	**NodeJS**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-48933, CVE-2026-48618, CVE-2026-48615, CVE-2026-48617, CVE-2026-48619, CVE-2026-48937, CVE-2026-48928, CVE-2026-48930, CVE-2026-48934, CVE-2026-48935, CVE-2026-48936, CVE-2026-48931)
Description	NodeJS has released a security update addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected systems. NodeJS advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	NodeJS Versions: • 26.x • 24.x • 22.x Dependencies: • llhttp (9.4.2) on all release lines • nghttp2 (1.69.0) on all release lines • openssl (3.5.7) on all release lines • undici (8.5.0) on 26.3.1 • undici (7.28.0) on 24.17.0 • undici (6.27.0) on 22.23.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://nodejs.org/en/blog/vulnerability/june-2026-security-releases

Vendor	**cPanel**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-42055, CVE-2026-48142, CVE-2026-48618, CVE-2026-48933, CVE-2026-48937, CVE-2026-48930, CVE-2026-48619, CVE-2026-48615, CVE-2026-48934, CVE-2026-48928, CVE-2026-48617, CVE-2026-48931, CVE-2026-48935)
Description	cPanel has a released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected systems. cPanel advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	EasyApache 4 • ea-nodejs22 - Versions 22.22.3 to 22.23.0 • ea-nginx - versions 1.31.1 to 1.31.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://docs.cpanel.net/changelogs/easyapache-4-change-log-25/

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.