Advisory Alert

Alert Number: AAA20260810 **Date:** August 10, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Vendor	Severity	Vulnerability
HPE	**Critical**	Authentication Middleware Header Handling Vulnerability
IBM	**Critical**	Multiple Vulnerabilities
Cisco	**High**	Multiple Vulnerabilities
IBM	**High**, **Medium**, **Low**	Multiple Vulnerabilities
HPE	**High**, **Medium**, **Low**	Multiple Vulnerabilities
SonicWall	**Medium**	Out-of-bounds Kernel Memory Read Vulnerability
F5	**Medium**	Security Update

Description

Vendor	**HPE**
Severity	**Critical**
Affected Vulnerability	Authentication Middleware Header Handling Vulnerability (CVE-2026-54763)
Description	HPE has released a security update addressing a vulnerability that exists in their products. **CVE-2026-54763:** Traefik is an HTTP reverse proxy and load balancer. Traefik's BasicAuth, DigestAuth, and ForwardAuth middlewares strip canonical-cased spoofed identity headers before writing Traefik's own value, but do not account for underscore-variant header names, which many backends normalize identically to dashed forms. An attacker able to reach a protected route can inject an underscore-variant header that survives Traefik's stripping and reaches the backend alongside, or on the unauthenticated ForwardAuth authResponseHeaders path instead of, the value Traefik intended to set, spoofing identity or authorization context. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	HPE Aruba Networking Private 5G Core version 1.26.1.2 and below
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw05119en_us&docLocale=en_US

Vendor	**IBM**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-4800, CVE-2026-33937, CVE-2026-10109, CVE-2026-42581, CVE-2026-42584)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected systems. IBM advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	IBM WebSphere eXtreme Scale versions 8.6.2.0 - 8.6.2.2 IBM Big SQL on IBM Cloud Pak for Data version 5.0 IBM Big SQL on IBM Software Hub versions 5.1, 5.2, 5.3 and 5.4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7282872 https://www.ibm.com/support/pages/node/7282929

Vendor	**Cisco**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-20337, CVE-2026-20338, CVE-2026-20339, CVE-2026-20345, CVE-2026-20346, CVE-2026-20347, CVE-2026-20348)
Description	Cisco 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. Cisco advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Secure Endpoint Connector for Linux, Mac and Windows Secure Endpoint Private Cloud versions prior to 4.2.8
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-clamav-WuuvVd26

Vendor	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-2950, CVE-2026-9002, CVE-2026-33939, CVE-2026-33916, CVE-2026-33938, CVE-2026-33940, CVE-2026-33941, CVE-2026-10543, CVE-2026-35091, CVE-2026-35092, CVE-2026-50020, CVE-2026-42578, CVE-2026-50560, CVE-2026-47244, CVE-2026-48043, CVE-2026-45416, CVE-2026-45205, CVE-2026-16480, CVE-2026-18097, CVE-2026-18096, CVE-2026-10534, CVE-2026-12143, CVE-2026-48779, CVE-2026-10051, CVE-2026-6790, CVE-2026-25645, CVE-2026-8384, CVE-2026-21932, CVE-2026-21945, CVE-2026-54399, CVE-2026-45149, CVE-2026-7771, CVE-2026-9762, CVE-2026-22021, CVE-2026-22013, CVE-2026-22007, CVE-2026-10695, CVE-2026-10535, CVE-2026-41417, CVE-2026-34479, CVE-2026-11906, CVE-2025-14813, CVE-2026-5598, CVE-2026-5588, CVE-2026-34480, CVE-2026-34477, CVE-2026-34478, CVE-2026-33871, CVE-2026-42583, CVE-2026-42580, CVE-2026-42585, CVE-2026-42587, CVE-2026-33870, CVE-2025-36372)
Description	IBM 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. IBM advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	IBM WebSphere eXtreme Scale versions 8.6.2.0 to 8.6.2.2 IBM Big SQL on IBM Cloud Pak for Data version 5.0 IBM Big SQL on IBM Software Hub versions 5.1, 5.2, 5.3 and 5.4 IBM Db2 Server versions 11.5.0 to 11.5.9 and 12.1.0 to 12.1.5 Decision Optimization for Cloud Pak for Data Version 5.4.0 before Patch 4 CPDS versions 1.0.0.0 to 1.0.10.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/bulletin/

Vendor	**HPE**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-35991, CVE-2025-31648, CVE-2022-23932, CVE-2026-33377)
Description	HPE has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected systems could be locally exploited to allow escalation of privilege vulnerability HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	HPE Cray XD670 Version Prior to 2.09 (HFP 2026.05.00)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf05068en_us&docLocale=en_US • https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf05067en_us&docLocale=en_US • https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf05066en_us&docLocale=en_US

Vendor	**SonicWall**
Severity	**Medium**
Affected Vulnerability	Out-of-bounds Kernel Memory Read Vulnerability (CVE-2026-66151)
Description	SonicWall has released a security update addressing a vulnerability that exists in their products. **CVE-2026-66151:** SonicWall Global VPN Client version 4.10.8.1108 and earlier is vulnerable to an out-of-bounds kernel memory read in the SWIPsec.sys driver, which could allow a local attacker to cause a system crash. SonicWall advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	SonicWall Global VPN Client (GVC) 4.10.8.1108 and earlier versions
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2026-0010

Vendor	**F5**
Severity	**Medium**
Affected Vulnerability	Security Update (CVE-2026-6472)
Description	F5 has released a security update addressing a vulnerability that exists in their products. **CVE-2026-6472:** Missing authorization in PostgreSQL CREATE TYPE allows an object creator to hijack other queries that use search_path to find user-defined types, including extension-defined types. That is to say, the victim will execute arbitrary SQL functions of the attacker's choice. F5 advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	BIG-IP Next for Kubernetes versions 2.3.0 and 2.0.0 to 2.2.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://my.f5.com/manage/s/article/K000162806

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.