Advisory Alert

Alert Number: AAA20260525 **Date:** May 25, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
F5	**Critical**	Heap Buffer Overflow Vulnerability
IBM	**Critical**	Multiple Vulnerabilities
NetApp	**High**	Linux Kernel PIE Stack Buffer Corruption Vulnerability
cPanel	**High**	Remote Code Execution Vulnerability
Ubuntu	**High**, Medium	Multiple Vulnerabilities
IBM	**High**, Medium, Low	Multiple Vulnerabilities

Description

Affected Product	**F5**
Severity	**Critical**
Affected Vulnerability	Heap buffer overflow Vulnerability (CVE-2026-9256)
Description	F5 has released a security update addressing a vulnerability that exist in their products. **CVE-2026-9256** - This vulnerability exists in the NGINX Plus and NGINX Open Source products. An unauthenticated attacker along with conditions beyond its control can exploit this vulnerability by sending crafted HTTP requests. This may cause a heap buffer overflow in the NGINX worker process leading to a restart. Additionally, for systems with Address Space Layout Randomization (ASLR) disabled, code execution is possible. F5 advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	NGINX Plus versions • 37.0.0 • R32 - R36 NGINX Open Source versions • 1.31.0 • 1.0.0 - 1.30.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://my.f5.com/manage/s/article/K000161377

Affected Product	**IBM**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-62718, CVE-2026-4800, CVE-2026-25896, CVE-2026-27962, CVE-2026-33896, CVE-2026-34520, CVE-2026-42043, CVE-2026-42044)
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 affected systems. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Watsonx Code Assistant On Prem Versions: • 5.1.1, 5.1.2, 5.1.3, 5.2, 5.2.1, 5.2.2, 5.3.0 and 5.3.1 patch 1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7273763

Affected Product	**NetApp**
Severity	**High**
Affected Vulnerability	Linux Kernel PIE Stack Buffer Corruption Vulnerability (CVE-2017-1000253)
Description	NetApp has released a security update addressing a vulnerability that exist in their products. **CVE-2017-1000253** - Certain versions of Linux kernel are susceptible to this vulnerability which when successfully exploited could lead to disclosure of sensitive information, addition or modification of data, or Denial of Service (DoS). NetApp advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	NetApp Cloud Backup (formerly AltaVault)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.netapp.com/advisory/ntap-20260522-0015

Affected Product	**cPanel**
Severity	**High**
Affected Vulnerability	Remote Code Execution Vulnerability (CVE-2026-9256)
Description	cPanel has released a security update addressing a vulnerability that exist in their products. **CVE-2026-9256** - An unauthenticated attacker along with conditions beyond their control can exploit this vulnerability by sending crafted HTTP requests. This may cause a heap buffer overflow in the NGINX worker process leading to a restart. Additionally, attackers can execute code on systems with Address Space Layout Randomization (ASLR) disabled or when the attacker can bypass ASLR. cPanel advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	EasyApache 4 • ea-nginx version 1.31.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://docs.cpanel.net/changelogs/easyapache-4-change-log-25/

Affected Product	**Ubuntu**
Severity	**High, Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-71088, CVE-2025-71090, CVE-2025-71127, CVE-2025-71134, CVE-2025-71139, CVE-2025-71141, CVE-2025-71142, CVE-2025-71144, CVE-2025-71152, CVE-2025-71155, CVE-2026-23274, CVE-2026-23351, CVE-2026-23394, CVE-2026-31419, CVE-2026-31431, CVE-2026-31504, CVE-2026-31533, CVE-2026-43033, CVE-2026-43077, CVE-2026-43078)
Description	Ubuntu has released a security update addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise affected systems. Ubuntu advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Ubuntu version 24.04 LTS
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-8277-2

Affected Product	**IBM**
Severity	**High, Medium, Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-1839, CVE-2026-2950, CVE-2026-4538, CVE-2026-4867, CVE-2026-22815, CVE-2026-26013, CVE-2026-26278, CVE-2026-28490, CVE-2026-33532, CVE-2026-33750, CVE-2026-33891, CVE-2026-33894, CVE-2026-33895, CVE-2026-34070, CVE-2026-34450, CVE-2026-34452, CVE-2026-34513, CVE-2026-34514, CVE-2026-34515, CVE-2026-34516, CVE-2026-34517, CVE-2026-34518, CVE-2026-34519, CVE-2026-34525, CVE-2026-40175, CVE-2026-42033, CVE-2026-42034, CVE-2026-42035, CVE-2026-42036, CVE-2026-42037, CVE-2026-42038, CVE-2026-42039, CVE-2026-42040, CVE-2026-42041, CVE-2026-42042)
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 affected systems. IBM advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	watsonx Code Assistant On Prem Versions: • 5.1.1, 5.1.2, 5.1.3, 5.2, 5.2.1, 5.2.2, 5.3.0 and 5.3.1 patch 1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7273763

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.