Advisory Alert

Alert Number: AAA20250526 **Date:** May 26, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Ivanti	**Critical**	Input Validation Vulnerability
NetApp	**High, Medium**	Multiple Vulnerabilities
F5	**Medium**	Information Disclosure Vulnerability
Broadcom VMware	**Medium**	SQL Injection Vulnerability

Description

Affected Product	**Ivanti**
Severity	**Critical**
Affected Vulnerability	Input Validation Vulnerability (CVE-2024-37404)
Description	Ivanti has released a security update addressing an Input Validation vulnerability affecting Connect Secure and Policy Secure products. **CVE-2024-37404 –** An input validation vulnerability in the CSR generation feature of Ivanti Connect Secure and Policy Secure allows an authenticated administrator to inject malicious configuration via CRLF injection, potentially leading to remote code execution with root privileges. Ivanti advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	• Ivanti Connect Secure - All versions before 22.7R2.1, 9.1R18.9 • Ivanti Policy Secure - All versions before 22.7R1.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Connect-Secure-and-Policy-Secure-CVE-2024-37404?language=en_US

Affected Product	**NetApp**
Severity	**High, Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-50083, CVE-2024-12133)
Description	NetApp has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2024-50083 -** A vulnerability in the Linux kernel before versions 5.10.228, 5.15.169, 6.1.114, 6.6.58, 6.11.5, and 6.12 allows a local attacker to cause a Denial of Service (DoS) by triggering a flaw that disrupts kernel operations, leading to system instability or crashes. **CVE-2024-12133 -** A vulnerability in GNU libtasn1 versions up to 4.19.0 that allows a local attacker to cause a Denial of Service (DoS) by exploiting a flaw in the ASN.1 parsing logic, resulting in system instability or crashes. NetApp advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	• E-Series SANtricity OS Controller Software 11.x • Active IQ Unified Manager for VMware vSphere
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://security.netapp.com/advisory/ntap-20250523-0010/ • https://security.netapp.com/advisory/ntap-20250523-0003/

Affected Product	**F5**
Severity	**Medium**
Affected Vulnerability	Information Disclosure Vulnerability (CVE-2022-40982)
Description	F5 has released a security update addressing an Information Disclosure vulnerability in Intel processors used in their rSeries platforms. **CVE-2022-40982 -** A speculative execution vulnerability in certain Intel processors may allow an authenticated local user to extract sensitive information from system memory. This issue, known as Downfall, leverages transient execution side-channel attacks to bypass typical isolation boundaries, potentially compromising data confidentiality in shared environments. F5 advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	F5OS-A - 1.7.0, 1.5.0 - 1.5.2, 1.4.0, 1.3.0 - 1.3.2 running on rSeries - r10600, r10800, r10900 (C128), r10920-DF (C137), r5600, r5800, r5900 (C129)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://my.f5.com/manage/s/article/K000135795

Affected Product	**Broadcom VMware**
Severity	**Medium**
Affected Vulnerability	SQL Injection Vulnerability (CVE-2025-41233)
Description	Broadcom has released a security update addressing an SQL Injection vulnerability in VMware Avi Load Balancer. **CVE-2025-41233 –** An authenticated blind SQL injection vulnerability in VMware Avi Load Balancer could allow a malicious user with network access to execute unauthorized SQL queries, potentially leading to information disclosure. Broadcom advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	VMware Avi Load Balancer - 30.1.1, 30.1.2, 30.2.1, 30.2.2, 30.2.3, 31.1.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/security-advisories/0/25707

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.