Advisory Alert

Alert Number: AAA20250721 **Date:** July 21, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
F5	**High**	Resource Exhaustion Vulnerability
Broadcom VMware	**High**	Multiple Cross-Site Scripting Vulnerabilities
NetApp	**Medium**	Security Update
Ubuntu	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**F5**
Severity	**High**
Affected Vulnerability	Resource Exhaustion Vulnerability (CVE-2025-21087)
Description	F5 has released a security update addressing a resource exhaustion vulnerability that exists in their product. **CVE-2025-21087** - When Client SSL or Server SSL profiles are configured on a virtual server, or Domain Name System Security Extensions (DNSSEC) signing operations are in use, undisclosed traffic can cause an increase in memory and CPU resource utilization. This vulnerability allows a remote, unauthenticated attacker to cause a degradation of service that can lead to a denial-of-service (DoS). F5 advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	BIG-IP (all modules) - 15.1.0 - 15.1.10, 16.1.0 - 16.1.5, 17.1.0 - 17.1.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://my.f5.com/manage/s/article/K000134888

Affected Product	**Broadcom VMware**
Severity	**High** - Initial release date **4th June 2025**
Affected Vulnerability	Multiple Cross-Site Scripting Vulnerabilities (CVE-2025-22243, CVE-2025-22244, CVE-2025-22245)
Description	Broadcom has released security updates addressing multiple cross-site scripting vulnerabilities that exist in their products. **CVE-2025-22243** - VMware NSX Manager UI is vulnerable to a stored Cross-Site Scripting (XSS) attack due to improper input validation. A malicious actor with privileges to create or modify network settings may be able to inject malicious code that gets executed when viewing the network settings. **CVE-2025-22244** - VMware NSX contains a stored Cross-Site Scripting (XSS) vulnerability in the gateway firewall due to improper input validation. A malicious actor with access to create or modify the response page for filtering URL may be able to inject malicious code that gets executed when another user tries to access the filtered website. **CVE-2025-22245** - VMware NSX contains a stored Cross-Site Scripting (XSS) vulnerability in the router port due to improper input validation. A malicious actor with privileges to create or modify router ports may be able to inject malicious code that gets executed when another user tries to access the router port. Broadcom advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	VMware NSX - 4.1.x, 4.0.x, 4.2.x NSX-T - 3.2.x VMware Cloud Foundation - 4.5.x ,5.1.x, 5.0.x ,5.2.x VMware Telco Cloud Infrastructure - 3.x, 2.x VMware Telco Cloud Platform - 5.x, 4.x, 3.x, 2.x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/security-advisories/0/25738

Affected Product	**NetApp**
Severity	**Medium**
Affected Vulnerability	Security Update (CVE-2025-21502)
Description	NetApp has released a security update addressing a vulnerability that exists in its products. **CVE-2025-21502** - Multiple NetApp products incorporate Oracle Java SE. Oracle Java SE versions 8u431-perf, 11.0.25, 17.0.13, 21.0.5, and 23.0.1 are susceptible to a vulnerability that allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE accessible data as well as unauthorized read access to a subset of Oracle Java SE accessible data. NetApp advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Data Infrastructure Insights Storage Workload Security Agent (formerly Cloud Insights Storage Workload Security Agent). OnCommand Workflow Automation
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.netapp.com/advisory/ntap-20250124-0009

Affected Product	**Ubuntu**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities
Description	Ubuntu has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected system. Ubuntu advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ubuntu 20.04 Ubuntu 22.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-7654-1

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.