Advisory Alert

Alert Number: AAA20240705 **Date:** July 5, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
NetApp	**High**	RegreSSHion Vulnerability
Apache HTTP Server	**High**	Source Code Disclosure
Apache Tomcat	**High**	Denial of Service Vulnerability
Ubuntu	**High**, Medium	Multiple Vulnerabilities
Hitachi	**High**, Medium, Low	Multiple Vulnerabilities
F5	Medium	Integrity Check Bypass Vulnerability

Description

Affected Product	**NetApp**
Severity	**High**
Affected Vulnerability	RegreSSHion Vulnerability (CVE-2024-6387)
Description	NetApp has released workarounds addressing the RegreSSHion vulnerability in its products which incorporate OpenSSH. Multiple OpenSSH versions are susceptible to a vulnerability referred to as regreSSHion which when successfully exploited could lead to disclosure of sensitive information, addition or modification of data, or Denial of Service. NetApp advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	E-Series SANtricity OS Controller Software 11.80.1 when ssh login is enabled.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.netapp.com/advisory/ntap-20240701-0001/

Affected Product	**Apache HTTP Server**
Severity	**High**
Affected Vulnerability	Source Code Disclosure (CVE-2024-39884)
Description	Apache has released security updates addressing a Source Code Disclosure Vulnerability that exists in Apache HTTP Server. A regression in the core of Apache HTTP Server 2.4.60 ignores some use of the legacy content-type based configuration of handlers. "AddType" and similar configuration, under some circumstances where files are requested indirectly, result in source code disclosure of local content. Apache advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Apache HTTP Server 2.4.60
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://httpd.apache.org/security/vulnerabilities_24.html

Affected Product	**Apache Tomcat**
Severity	**High**
Affected Vulnerability	Denial of Service Vulnerability (CVE-2024-34750)
Description	Apache has released security updates addressing a Denial of Service Vulnerability that exists in Apache Tomcat. When processing an HTTP/2 stream, Tomcat did not handle some cases of excessive HTTP headers correctly. This led to a miscounting of active HTTP/2 streams which in turn led to the use of an incorrect infinite timeout which allowed connections to remain open which should have been closed. Apache advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Apache Tomcat versions 11.0.0-M1 to 11.0.0-M20 Apache Tomcat versions 10.1.0-M1 to 10.1.24 Apache Tomcat versions 9.0.0-M1 to 9.0.89
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://tomcat.apache.org/security-11.html • https://tomcat.apache.org/security-10.html • https://tomcat.apache.org/security-9.html

Affected Product	**Ubuntu**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-21823, CVE-2024-26924, CVE-2024-26643, CVE-2024-26925, CVE-2024-26924, CVE-2024-26809)
Description	Ubuntu has released security updates addressing multiple vulnerabilities that exist in Ubuntu Linux kernel. 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 24.04 Ubuntu 23.10 Ubuntu 22.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://ubuntu.com/security/notices/USN-6864-2 • https://ubuntu.com/security/notices/USN-6872-2

Affected Product	**Hitachi**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities
Description	Hitachi has released security updates addressing multiple vulnerabilities that exist in Hitachi Disk Array Systems. Exploitation of these vulnerabilities may lead to Privilege Escalation, Remote Code Execution, Security Bypass, Information Disclosure. Hitachi advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Hitachi Virtual Storage Platform 5200, 5600, 5200H, 5600H, 5100, 5500, 5100H, 5500H, G1000, G1500, F1500, VX7
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.hitachi.com/products/it/storage-solutions/sec_info/2024/04.html

Affected Product	**F5**
Severity	**Medium**
Affected Vulnerability	Integrity Check Bypass Vulnerability (CVE-2023-48795)
Description	F5 has released security updates addressing an Integrity Check Bypass Vulnerability that exists in third party products that are used in F5OS and Traffix SDC. This vulnerability allows an attacker with the ability to intercept SSH traffic to downgrade connection security and force the usage of less secure client authentication algorithms. F5 advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	F5OS-A versions 1.7.0 and 1.5.1 - 1.5.2 F5OS-C versions 1.6.0 - 1.6.2 Traffix SDC versions 5.2.0 and 5.1.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://my.f5.com/manage/s/article/K000138264

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind. FinCSIRT highly recommend to follow the company policies and procedures when applying the necessary patches with thorough testing and ensuring proper roll-back capabilities exists.