Advisory Alert

Alert Number: AAA20240826 **Date:** August 26, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
F5	**High**	Null Pointer Dereference Vulnerability
NetApp	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**F5**
Severity	**High**
Affected Vulnerability	Null Pointer Dereference Vulnerability (CVE-2024-38477)
Description	F5 has released security updates addressing a Null Pointer Dereference Vulnerability that exists in Apache HTTP Server 2.4.59 and earlier that affects F5 products. This vulnerability could allow an attacker to crash the server via a malicious request. F5 advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	BIG-IP (all modules) - Versions 17.1.0 - 17.1.1, 16.1.0 - 16.1.5, 15.1.0 - 15.1.10 F5OS-A - Versions 1.7.0, 1.5.1 - 1.5.2 F5OS-C - Versions 1.6.0 - 1.6.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://my.f5.com/manage/s/article/K000140784

Affected Product	**NetApp**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-4741, CVE-2023-6237)
Description	NetApp has released security updates addressing multiple vulnerabilities that exist in OpenSSL that in turn affect NetApp products. **CVE-2024-4741**- Multiple NetApp products incorporate OpenSSL. OpenSSL versions 3.3, 3.2, 3.1, 3.0 and 1.1.1 are susceptible to a vulnerability which when successfully exploited could lead to disclosure of sensitive information, addition or modification of data, or Denial of Service (DoS). **CVE-2023-6237**- Multiple NetApp products incorporate OpenSSL. OpenSSL versions 3.0.0 prior to 3.0.13, 3.1.0 prior to 3.1.5 and 3.2.0 are susceptible to a vulnerability which when successfully exploited could lead to Denial of Service (DoS). NetApp advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	NetApp HCI Baseboard Management Controller (BMC) - H615C, H610S, H610C
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://security.netapp.com/advisory/ntap-20240621-0004/ • https://security.netapp.com/advisory/ntap-20240531-0007/

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.