Advisory Alert

Alert Number: **AAA20241025** **Date:** **October 25, 2024**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
NetApp	**Critical**	Buffer Underwrite Vulnerability
IBM	**High**, **Medium**, **Low**	Multiple Vulnerabilities
F5	**High**, **Medium**	Use-after-free Vulnerability

Description

Affected Product	**NetApp**
Severity	**Critical**
Affected Vulnerability	Buffer Underwrite Vulnerability (CVE-2024-45490)
Description	NetApp has released security updates addressing a Buffer Underwrite Vulnerability that exists in libexpat library which is incorporated by NetApp products. **CVE-2024-45490** - Libexpat versions prior to 2.6.3 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). NetApp advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	ONTAP 9
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.netapp.com/advisory/ntap-20241018-0004/

Affected Product	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2019-19012,CVE-2019-13224,CVE-2019-16163,CVE-2022-24736,CVE-2022-24735,CVE-2022-24834,CVE-2023-45145,CVE-2023-28856,CVE-2024-6345,CVE-2024-35195,CVE-2024-5569,CVE-2024-37891,CVE-2024-39689,CVE-2024-34064)
Description	IBM has released security updates addressing Multiple Vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause heap-based buffer overflow, denial of service, cross-site scripting, sensitive information disclosure. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM QRadar Assistant 1.0.0 - 3.8.0 IBM SOAR QRadar Plugin App 1.0.0 - 5.4.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7174015 • https://www.ibm.com/support/pages/node/7174016

Affected Product	**F5**
Severity	**High**, **Medium**
Affected Vulnerability	Use-after-free Vulnerability (CVE-2024-25062)
Description	F5 has released security updates addressing a Use-after-free Vulnerability that exist in their products. **CVE-2024-25062** - An issue was discovered in libxml2 before 2.11.7 and 2.12.x before 2.12.5. When using the XML Reader interface with DTD validation and XInclude expansion enabled, processing crafted XML documents can lead to an xmlValidatePopElement use-after-free. F5 advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	BIG-IP Next SPK 1.7.0 - 1.9.2 BIG-IP Next CNF 1.1.0 - 1.3.1 BIG-IP (all modules) 17.1.0 - 17.1.1 BIG-IP (all modules) 16.1.0 - 16.1.5 BIG-IP (all modules) 15.1.0 - 15.1.10
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://my.f5.com/manage/s/article/K000141357

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.