Advisory Alert

Alert Number: AAA20240304 **Date:** March 4, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Juniper	**Critical**	Multiple Vulnerabilities
F5	**High**	Out-Of-Bounds Write Vulnerability

Description

Affected Product	**Juniper**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-43552, CVE-2023-44981, CVE-2023-5676, CVE-2023-43642, CVE-2023-32360, CVE-2022-40982, CVE-2023-3611, CVE-2023-3776, CVE-2023-4206, CVE-2023-4207, CVE-2023-4208, CVE-2023-20593, CVE-2023-20569, CVE-2023-37920)
Description	Juniper has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities could lead to Use-after-free condition, Privilege escalation, Information disclosure, Out-of-bounds writes. Juniper recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Juniper Secure Analytics (JSA) all versions prior to 7.5.0 UP7
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://supportportal.juniper.net/s/article/On-Demand-JSA-Series-Multiple-vulnerabilities-resolved-in-Juniper-Secure-Analytics-in-7-5-0-UP7-IF05?language=en_US

Affected Product	**F5**
Severity	**High**
Affected Vulnerability	Out-Of-Bounds Write Vulnerability (CVE-2023-3611)
Description	F5 has released a security update addressing an Out-of-bounds write vulnerability. An attacker may exploit this vulnerability to disclose sensitive information, modify data, or cause a denial-of-service (DoS). F5 recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	F5 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/K000138726

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.