Advisory Alert

Alert Number: AAA20240129 **Date:** January 29, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Juniper	**Critical**	Out-of-bounds Write Vulnerability
Red Hat	**High**	HTTP request smuggling Vulnerability
NetApp	**High**	Privilege Escalation Vulnerability
IBM	**High**, **Medium**, **Low**	Multiple Vulnerabilities

Description

Affected Product	**Juniper**
Severity	**Critical**
Affected Vulnerability	Out-of-bounds Write Vulnerability (CVE-2024-21591)
Description	Juniper has released a security update for an Out-of-bounds Write Vulnerability that exist in Juniper Junos OS. The vulnerability exists in J-Web of Juniper Networks Junos OS SRX Series and EX Series allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS), or Remote Code Execution (RCE) and obtain root privileges on the device. Juniper recommends to apply the necessary security updates at earliest to avoid issues.
Affected Products	Junos OS versions earlier than 20.4R3-S9 Junos OS 21.2 versions earlier than 21.2R3-S7 Junos OS 21.3 versions earlier than 21.3R3-S5 Junos OS 21.4 versions earlier than 21.4R3-S5 Junos OS 22.1 versions earlier than 22.1R3-S4 Junos OS 22.2 versions earlier than 22.2R3-S3 Junos OS 22.3 versions earlier than 22.3R3-S2 Junos OS 22.4 versions earlier than 22.4R2-S2, 22.4R3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://supportportal.juniper.net/s/article/2024-01-Security-Bulletin-Junos-OS-SRX-Series-and-EX-Series-Security-Vulnerability-in-J-web-allows-a-preAuth-Remote-Code-Execution-CVE-2024-21591?language=en_US

Affected Product	**Red Hat**
Severity	**High**
Affected Vulnerability	HTTP request smuggling Vulnerability (CVE-2023-46589)
Description	Red Hat has released a security patch updates addressing a HTTP request smuggling Vulnerability that exist in Apache Tomcat that in turn affects Red Hat products. Red Hat recommends to apply the necessary patch updates at your earliest to avoid issues.
.Affected Products	Red Hat Enterprise Linux for x86_64 - Extended Update Support 8.8 x86_64 Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 8.8 s390x Red Hat Enterprise Linux for Power, little endian - Extended Update Support 8.8 ppc64le Red Hat Enterprise Linux for ARM 64 - Extended Update Support 8.8 aarch64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2024:0532

Affected Product	**NetApp**
Severity	**High**
Affected Vulnerability	Privilege Escalation Vulnerability (CVE-2024-21985)
Description	NetApp has released security updates addressing a Privilege Escalation Vulnerability that exists in ONTAP 9. The vulnerability may allow an authenticated user with multiple remote accounts with differing roles to perform actions via REST API beyond their intended privilege. Possible actions include viewing limited configuration details and metrics or modifying limited settings, some of which could result in a Denial of Service (DoS). It is recommends to apply the necessary remediation at your earliest to avoid issues.
Affected Products	NetApp ONTAP 9 (formerly Clustered Data ONTAP)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.netapp.com/advisory/ntap-20240126-0001/

Affected Product	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-27538, CVE-2023-32681, CVE-2023-1410, CVE-2022-43552, CVE-2023-46159, CVE-2018-14041, CVE-2018-20677, CVE-2023-2801, CVE-2023-44487, CVE-2018-20676, CVE-2023-2183)
Description	IBM has released security updates addressing Multiple Vulnerabilities that exist in Storage Ceph. Successful exploitation of the above vulnerabilities could lead to Sensitive Information Disclosure, Use After Free condition, Denial of Service, Cross Site Scripting IBM recommends to apply the necessary patch updates at your earliest to avoid issues.
.Affected Products	IBM Storage Ceph <6.1 IBM Storage Ceph <6.1z3 IBM Storage Ceph 5.3z1-z3, 5.3z1-z5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7112257 https://www.ibm.com/support/pages/node/7112260 https://www.ibm.com/support/pages/node/7112261 https://www.ibm.com/support/pages/node/7112262 https://www.ibm.com/support/pages/node/7112263 https://www.ibm.com/support/pages/node/7112264 https://www.ibm.com/support/pages/node/7112265 https://www.ibm.com/support/pages/node/7112266 https://www.ibm.com/support/pages/node/7112267 https://www.ibm.com/support/pages/node/7112268 https://www.ibm.com/support/pages/node/7112269

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.