Advisory Alert

Alert Number: AAA20240118 **Date:** January 18, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Juniper	**Critical**	Multiple Vulnerabilities
HPE	**Critical**	Multiple Vulnerabilities
Dell	**High**	Multiple Vulnerabilities
SUSE	**High**	Multiple Vulnerabilities
IBM	**High**, Medium	Multiple Vulnerabilities

Description

Affected Product	**Juniper**
Severity	**Critical**
Affected Vulnerability	Multiple vulnerabilities (CVE-2022-40152, CVE-2023-34058, CVE-2023-34059, CVE-2023-40217, CVE-2023-50164, CVE-2023-50950)
Description	Juniper has released a security update addressing multiple vulnerabilities that exist in Juniper Secure Analytics. If exploited, these vulnerabilities could lead to denial of service, privilege escalation, Remote Code Execution Juniper recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Juniper Secure Analytics All versions up through 7.5.0 UP7 IF04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://supportportal.juniper.net/s/article/2024-01-Security-Bulletin-JSA-Series-Multiple-vulnerabilities-resolved?language=en_US

Affected Product	**HPE**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities(CVE-2023-45802, CVE-2023-43622, CVE-2023-31122, CVE-2006-20001, CVE-2022-36760, CVE-2022-37436, CVE-2023-25690, CVE-2023-27522)
Description	HPE has released a security update addressing multiple vulnerabilities that exist in HP-UX Apache Web Server. If exploited, these vulnerabilities could lead to Access Restriction Bypass, Disclosure of Information, Server-Side Request Forgery, Memory corruption. HPE highly recommends to apply necessary security patches at earliest to avoid issues
Affected Products	HP-UX Apache-based Web Server Prior to B.2.4.58.00
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbux04589en_us

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-45229, CVE-2023-45230, CVE-2023-45231, CVE-2023-45232, CVE-2023-45233, CVE-2023-45234, CVE-2023-45235, CVE-2023-45236, CVE-2023-45237)
Description	Dell has released a security update addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected system. Dell recommends to apply the necessary patch updates at your earliest to avoid issues.
.Affected Products	Multiple Dell PowerEdge products Dell XC series Multiple Dell Storage NX products Multiple Dell EMC products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000220253/dsa-2023-357-security-update-for-dell-poweredge-server-bios-for-tianocore-edk2-vulnerabilities

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2020-26555, CVE-2023-51779, CVE-2023-6121, CVE-2023-6606, CVE-2023-6610, CVE-2023-6931, CVE-2023-6932, CVE-2022-45887, CVE-2023-1206, CVE-2023-31085, CVE-2023-3111, CVE-2023-39189, CVE-2023-39192, CVE-2023-39193, CVE-2023-39197, CVE-2023-45863)
Description	SUSE has released security updates addressing multiple vulnerabilities in products. If exploited, these vulnerabilities could lead to escalation of privilege, denial of service, information leak. SUSE recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	SUSE Linux Enterprise Server 11 SP4, 11 SP4 LTSS EXTREME CORE 11-SP4 SUSE Linux Enterprise Micro 5.1, 5.2 SUSE Linux Enterprise Micro for Rancher 5.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2024/suse-su-20240110-1/ https://www.suse.com/support/update/announcement/2024/suse-su-20240112-1/

Affected Product	**IBM**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-34058, CVE-2023-34059, CVE-2022-40152, CVE-2023-40217, CVE-2023-50950, CVE-2023-50164)
Description	IBM has released a security update addressing multiple vulnerabilities that exists in their products. If exploited these vulnerabilities could lead to sensitive information disclosure ,denial of service, privilege escalation It is recommended by IBM to apply necessary security fixes at earliest to avoid issues
.Affected Products	IBM QRadar SIEM 7.5 - 7.5.0 UP7
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7108657

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.