Advisory Alert

Alert Number: AAA20240806 **Date:** August 6, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
IBM	**Critical**	Multiple Vulnerabilities
Juniper	**High**	Improper Check for Unusual or Exceptional Conditions Vulnerability
Dell	**High**	Multiple Vulnerabilities
SUSE	**High**	Multiple Vulnerabilities
IBM	**High**, Medium, Low	Multiple Vulnerabilities

Description

Affected Product	**IBM**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-50447, CVE-2023-49569)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected system. **CVE-2023-50447** - Pillow could allow a remote attacker to execute arbitrary code on the system, caused by improper neutralization of user supplied-input by the PIL.ImageMath.eval function. By sending a specially crafted request using keys that leverage the environment parameter, an attacker could exploit this vulnerability to execute arbitrary code on the system. **CVE-2023-49569** - go-git could allow a remote attacker to traverse directories on the system. By sending a specially crafted request using the ChrootOS, an attacker could exploit this vulnerability to create and amend files across the filesystem and possibly execute arbitrary code on the system. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Storage Ceph 7.0-7.0z2 IBM Storage Ceph 6.0, 6.1-6.1z6 IBM Storage Ceph 5.3-5.3z6
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7160168 • https://www.ibm.com/support/pages/node/7162569

Affected Product	**Juniper**
Severity	**High**
Affected Vulnerability	Improper Check for Unusual or Exceptional Conditions Vulnerability (CVE-2024-39545)
Description	Juniper has released security updates addressing an Unusual or Exceptional Conditions Vulnerability that exists in their products. **CVE-2024-39545** - An Improper Check for Unusual or Exceptional Conditions vulnerability in the the IKE daemon (iked) of Juniper Networks Junos OS on SRX Series, MX Series with SPC3 and NFX350 allows an unauthenticated, network-based attacker sending specific mismatching parameters as part of the IPsec negotiation to trigger an iked crash leading to Denial of Service (DoS). Juniper advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	This issue affects Junos OS on SRX Series, MX Series with SPC3 and NFX350 running iked : • All versions before 21.2R3-S8, • from 21.4 before 21.4R3-S7, • from 22.1 before 22.1R3-S2, • from 22.2 before 22.2R3-S1, • from 22.3 before 22.3R2-S1, 22.3R3, • from 22.4 before 22.4R1-S2, 22.4R2, 22.4R3.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://supportportal.juniper.net/s/article/2024-07-Security-Bulletin-Junos-OS-SRX-Series-and-MX-Series-with-SPC3-and-NFX350-When-VPN-tunnels-parameters-are-not-matching-the-iked-process-will-crash-CVE-2024-39545?language=en_US

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-31355, CVE-2024-21978, CVE-2024-21980)
Description	Dell has released security updates addressing multiple vulnerabilities that exist in third-party products that in turn affect Dell products. These vulnerabilities could be exploited by malicious users to compromise the affected system. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	PowerEdge R6615 BIOS Versions prior to 1.8.3 PowerEdge R7615 BIOS Versions prior to 1.8.3 PowerEdge R6625 BIOS Versions prior to 1.8.3 PowerEdge R7625 BIOS Versions prior to 1.8.3 PowerEdge C6615 BIOS Versions prior to 1.3.3 PowerEdge R6515 BIOS Versions prior to 2.16.0 PowerEdge R6525 BIOS Versions prior to 2.16.2 PowerEdge R7515 BIOS Versions prior to 2.16.0 PowerEdge R7525 BIOS Versions prior to 2.16.2 PowerEdge C6525 BIOS Versions prior to 2.16.1 PowerEdge XE8545 BIOS Versions prior to 2.15.1 Dell EMC XC Core XC7525 BIOS Versions prior to 2.16.2 Dell XC Core XC7625 BIOS Versions prior to 1.8.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000227518/dsa-2024-306-security-update-for-dell-amd-based-poweredge-server-vulnerabilities

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-27398,CVE-2024-35950,CVE-2022-48651,CVE-2024-26610,CVE-2024-26828,CVE-2024-26852,CVE-2024-26923,CVE-2024-27398,CVE-2021-46955,CVE-2021-47383,CVE-2023-1829,CVE-2023-6531,CVE-2023-6546,CVE-2024-23307,CVE-2023-52502,CVE-2024-26930)
Description	SUSE has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Use after free conditions, Memory corruption, Race conditions. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	openSUSE Leap 15.3 openSUSE Leap 15.5 SUSE Linux Enterprise High Performance Computing 15 SP2, 15 SP3, 15 SP5 SUSE Linux Enterprise Live Patching 15 SP2, 15 SP3, 15 SP5 SUSE Linux Enterprise Micro 5.1, 5.2, 5.3 SUSE Linux Enterprise Real Time 15 SP5 SUSE Linux Enterprise Server 15 SP2, 15 SP3, 15 SP5 SUSE Linux Enterprise Server for SAP Applications 15 SP2, 15 SP3, 15 SP5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2024/suse-su-20242724-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20242725-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20242726-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20242740-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20242734-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20242751-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20242750-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20242755-1

Affected Product	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-49083,CVE-2023-27043,CVE-2023-39615,CVE-2023-2650,CVE-2023-3446,CVE-2023-4807,CVE-2023-28486,CVE-2024-2961,CVE-2021-41089,CVE-2022-24769,CVE-2021-41091,CVE-2018-20699,CVE-2022-36109,CVE-2024-33600,CVE-2023-5981,CVE-2024-0553,CVE-2023-42465,CVE-2021-35937,CVE-2023-45143,CVE-2022-25912,CVE-2022-25860,CVE-2022-25908,CVE-2023-7104,CVE-2024-0567,CVE-2023-38546,CVE-2021-35938,CVE-2024-1442,CVE-2018-20677,CVE-2018-20676,CVE-2019-8331,CVE-2018-14042,CVE-2018-14040,CVE-2016-10735,CVE-2023-4911,CVE-2021-35939,CVE-2022-25881,CVE-2024-33602,CVE-2022-40898,CVE-2024-25629,CVE-2024-33601,CVE-2022-40897,CVE-2023-43804,CVE-2024-24786,CVE-2024-4603,CVE-2024-2511,CVE-2023-49568)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Denial of service, Sensitive information disclosure, Privilege escalation, Cross-site scripting. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Storage Ceph 5.3z1-z6 IBM Storage Ceph 6.1-6.1z6, 6.0 IBM Storage Ceph 6.1z1-z6, 6.1, 6.0 IBM Storage Ceph 7.0-7.0z2 IBM MaaS360 VPN Module 2.89.000 - 3.000.800
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7160783 • https://www.ibm.com/support/pages/node/7160794 • https://www.ibm.com/support/pages/node/7160798 • https://www.ibm.com/support/pages/node/7160799 • https://www.ibm.com/support/pages/node/7160800 • https://www.ibm.com/support/pages/node/7162087 • https://www.ibm.com/support/pages/node/7162178 • https://www.ibm.com/support/pages/node/7162179 • https://www.ibm.com/support/pages/node/7162180 • https://www.ibm.com/support/pages/node/7162181 • https://www.ibm.com/support/pages/node/7162182 • https://www.ibm.com/support/pages/node/7162183 • https://www.ibm.com/support/pages/node/7162184 • https://www.ibm.com/support/pages/node/7162187 • https://www.ibm.com/support/pages/node/7162188 • https://www.ibm.com/support/pages/node/7162478 • https://www.ibm.com/support/pages/node/7162483 • https://www.ibm.com/support/pages/node/7162486 • https://www.ibm.com/support/pages/node/7162488 • https://www.ibm.com/support/pages/node/7162507 • https://www.ibm.com/support/pages/node/7162529 • https://www.ibm.com/support/pages/node/7162537 • https://www.ibm.com/support/pages/node/7162540 • https://www.ibm.com/support/pages/node/7162545 • https://www.ibm.com/support/pages/node/7162550 • https://www.ibm.com/support/pages/node/7162554 • https://www.ibm.com/support/pages/node/7162556 • https://www.ibm.com/support/pages/node/7162559 • https://www.ibm.com/support/pages/node/7162561 • https://www.ibm.com/support/pages/node/7162569 • https://www.ibm.com/support/pages/node/7162573 • https://www.ibm.com/support/pages/node/7162615

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.