Advisory Alert

Alert Number: **AAA20240419** **Date:** **April 19, 2024**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
Citrix	**High**	Privilege Escalation Vulnerability
Suse	**High**	Multiple Vulnerabilities
Ivanti	**High**	Multiple Vulnerabilities
Lenovo	**Medium**	Multiple Privilege Escalation Vulnerabilities
F5	**Medium**	Multiple Vulnerabilities
Juniper	**Medium**	Information Exposure Vulnerability

Description

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities
Description	Dell has released security updates addressing multiple vulnerabilities that exist in third party products that in turn affect Dell products. Malicious users could exploit these vulnerabilities to compromise the affected system. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Dell EMC VxRail Appliance 8.0.x versions prior to 8.0.211 Dell SmartFabric OS1 10.5.5.8
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000224302/dsa-2024-178-security-update-for-dell-vxrail-8-0-211-multiple-third-party-component-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000224301/dsa-2024-185-security-update-for-dell-os10-third-party-vulnerabilities

Affected Product	**Citrix**
Severity	**High**
Affected Vulnerability	Privilege Escalation Vulnerability (CVE-2024-3902)
Description	Citrix has released security updates addressing a Privilege Escalation Vulnerability that exists in Citrix uberAgent. Citrix advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Citrix uberAgent before 7.1.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.citrix.com/article/CTX635002/citrix-uberagent-security-bulletin-for-cve20243902

Affected Product	**Suse**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
Description	Suse has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities may lead to Null pointer dereference, Use-after-free, Memory corruption, Information leakage. Suse advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	openSUSE Leap 15.5 Public Cloud Module 15-SP5 SUSE Linux Enterprise High Performance Computing 15 SP5 SUSE Linux Enterprise Live Patching 15-SP5 SUSE Linux Enterprise Micro 5.5 SUSE Linux Enterprise Real Time 15 SP5 SUSE Linux Enterprise Server 15 SP5 SUSE Linux Enterprise Server for SAP Applications 15 SP5 SUSE Real Time Module 15-SP5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2024/suse-su-20241332-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20241322-2/ • https://www.suse.com/support/update/announcement/2024/suse-su-20241332-2/

Affected Product	**Ivanti**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-39340, CVE-2023-41719, CVE-2023-41720)
Description	Ivanti has released security updates addressing multiple vulnerabilities that exist their products. Exploitation of these vulnerabilities could lead to Denial of Service (DoS), Remote code execution and Privilege escalation. **CVE-2023-39340** - A vulnerability exists on both branches of Ivanti Connect Secure (9.1Rx and 22x) below 22.6R2 or 9.1R18.2 where an attacker can send a specific request which may lead to Denial of Service (DoS) of the appliance. **CVE-2023-41719** - A vulnerability exists on both branches of Ivanti Connect Secure (9.1Rx and 22x) below 22.6R2 or 9.1R18.5 where an attacker impersonating an administrator may craft a specific web request which may lead to remote code execution. **CVE-2023-41720** - A vulnerability exists on the 22x branch of Ivanti Connect Secure below 22.6R2 where an attacker can escalate their privileges by exploiting a vulnerable installed application. This vulnerability allows the attacker to gain elevated execution privileges on the affected system. Ivanti advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ivanti-Connect-Secure • All minor versions of 9.1Rx below the following (9.1R14.6, 9.1R15.4, 9.1R16.4 ,9.1R17.4, 9.1R18.5) • All minor versions of 22.x below the following (22.1R6.2, 22.2R4.2, 22.3R1.2, 22.4R1.1, 22.4R2.4, 22.5R1.3, 22.5R2.4, 22.6R1.2, 22.6R2.3) • All versions of 9.1Rx below 9.1R18.5 • All minor versions of 22.x below the following (22.6R2.2, 22.5R2.3, 22.4R1.1, 22.5R1.3) • All minor versions of 22.x below the following (22.4R2.4, 22.5R2.3, 22.6R2.3)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://forums.ivanti.com/s/article/Security-patch-release-Ivanti-Connect-Secure-22-6R2-and-22-6R2-1?language=en_US

Affected Product	**Lenovo**
Severity	**Medium**
Affected Vulnerability	Multiple Privilege Escalation Vulnerabilities (CVE-2023-31271, CVE-2023-32646, CVE-2023-34315)
Description	Lenovo has released security updates addressing multiple Privilege Escalation Vulnerabilities that exist in Intel Virtual RAID on CPU (VROC) software that in turn affect Lenovo products. Lenovo advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	MX3330-F All-flash Appliance (ThinkAgile) MX3330-H Hybrid Appliance (ThinkAgile) MX3331-F All-flash Certified node (ThinkAgile) MX3331-H Hybrid Certified node (ThinkAgile) DN8848 V2 (ThinkServer) SR588 V2 (ThinkServer) SR590 V2 (ThinkServer) SD630 V2 (ThinkSystem) SD650 V2 (ThinkSystem) SD650-N V2 (ThinkSystem) SN550 V2 (ThinkSystem) SR630 V2 (ThinkSystem) SR630 V3 (ThinkSystem) SR650 V2 (ThinkSystem) SR650 V3 (ThinkSystem) SR670 V2 (ThinkSystem) SR850 V2 (ThinkSystem) SR850 V3 (ThinkSystem) SR860 V2 (ThinkSystem) SR860 V3 (ThinkSystem) ST650 V2 (ThinkSystem) ST650 V3 (ThinkSystem) ST658 V2 (ThinkSystem) ST658 V3 (ThinkSystem)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.lenovo.com/us/en/product_security/LEN-154269

Affected Product	**F5**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-5981, CVE-2024-0553)
Description	F5 has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2023-5981**- A vulnerability was found that the response times to malformed ciphertexts in RSA-PSK ClientKeyExchange differ from response times of ciphertexts with correct PKCS#1 v1.5 padding. **CVE-2024-0553** - A vulnerability was found in GnuTLS. The response times to malformed ciphertexts in RSA-PSK ClientKeyExchange differ from the response times of ciphertexts with correct PKCS#1 v1.5 padding. This issue may allow a remote attacker to perform a timing side-channel attack in the RSA-PSK key exchange, potentially leading to the leakage of sensitive data. F5 advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	BIG-IP Next (all modules) 20.0.1 - 20.0.2 BIG-IP Next Central Manager 20.0.1 - 20.0.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://my.f5.com/manage/s/article/K000138649

Affected Product	**Juniper**
Severity	**Medium**
Affected Vulnerability	Information Exposure Vulnerability (CVE-2020-1628)
Description	Juniper has released security updates addressing an Information Exposure Vulnerability that exists in their products. It was discovered that packets utilizing the 128.0.0.0/2 subnet for internal communications between the RE and PFEs may egress an EX4300 or MX204, leaking configuration information such as heartbeats, kernel versions, etc. out to the Internet. Juniper advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Juniper Networks Junos OS: • 14.1X53 versions prior to 14.1X53-D53 on EX4300 • 15.1 versions prior to 15.1R7-S6 on EX4300 • 15.1X49 versions prior to 15.1X49-D200, 15.1X49-D210 on EX4300 • 16.1 versions prior to 16.1R7-S7 on EX4300 • 17.1 versions prior to 17.1R2-S11, 17.1R3-S2 on EX4300 • 17.2 versions prior to 17.2R3-S3 on EX4300 • 17.3 versions prior to 17.3R2-S5, 17.3R3-S7 on EX4300 • 17.4 versions prior to 17.4R2-S9, 17.4R3 on EX4300 • 18.1 versions prior to 18.1R3-S8 on EX4300 • 18.2 versions prior to 18.2R3-S2 on EX4300 • 18.3 versions prior to 18.3R2-S3, 18.3R3, 18.3R3-S1 on EX4300 • 18.4 versions prior to 18.4R1-S5, 18.4R2-S3, 18.4R3 on EX4300 • 19.1 versions prior to 19.1R1-S4, 19.1R2 on EX4300 • 19.2 versions prior to 19.2R1-S4, 19.2R2 on EX4300 • 19.3 versions prior to 19.3R1-S1, 19.3R2 on EX4300 • All versions prior to 20.4R3-S4 on MX204 • 21.4 versions prior to 21.4R1-S1, 21.4R2 on MX204
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://supportportal.juniper.net/s/article/2020-04-Security-Bulletin-Junos-OS-EX4300-and-MX204-Traffic-from-the-network-internal-to-the-device-128-0-0-0-may-be-forwarded-to-egress-interfaces-CVE-2020-1628?language=en_US

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.