TLP: WHITE

Advisory Alert

Alert Number: AAA20240918 **Date:** September 18, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

	Severity	Vulnerability
Broadcom VMware	**Critical**	Multiple Vulnerabilities
Ivanti	**Critical**	Insufficient Authorization Vulnerability
SolarWinds	**Critical**	Remote Code Execution Vulnerability
HPE	**High**	Multiple Vulnerabilities
Dell	**High**	Multiple Vulnerabilities
SUSE	**High**	Multiple Vulnerabilities
F5	**High**	Multiple Vulnerabilities
IBM	**High**, Medium	Multiple Vulnerabilities
Ubuntu	**High**, Medium, Low	Multiple Vulnerabilities
Cisco	**Medium**	Command Injection Vulnerability
Red Hat	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**Broadcom VMware**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-38812, CVE-2024-38813)
Description	Broadcom has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2024-38812** - The vCenter Server contains a heap-overflow vulnerability in the implementation of the DCERPC protocol. A malicious actor with network access to vCenter Server may trigger this vulnerability by sending a specially crafted network packet potentially leading to remote code execution. **CVE-2024-38813 -** The vCenter Server contains a privilege escalation vulnerability. A malicious actor with network access to vCenter Server may trigger this vulnerability to escalate privileges to root by sending a specially crafted network packet. Broadcom advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	VMware vCenter Server - 7.0, 8.0 VMware Cloud Foundation - 5.x, 4.x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/24968

Affected Product	**Ivanti**
Severity	**Critical**
Affected Vulnerability	Insufficient Authorization Vulnerability (CVE-2024-36130)
Description	Ivanti has released security updates addressing an Insufficient Authorization Vulnerability that exists in their products. **CVE-2024-36130 -** An insufficient authorization vulnerability in web component of EPMM prior to 12.1.0.1 allows an unauthorized attacker within the network to execute arbitrary commands on the underlying operating system of the appliance. Ivanti advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ivanti Endpoint Manager Mobile prior to 12.1.0.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Endpoint-Manager-for-Mobile-EPMM-July-2024?language=en_US

Affected Product	**SolarWinds**
Severity	**Critical**
Affected Vulnerability	Remote Code Execution Vulnerability (CVE-2024-28991)
Description	SolarWinds has released security updates addressing a Remote Code Execution Vulnerability that exists in their products. CVE-2024-28991 - SolarWinds Access Rights Manager (ARM) was found to be susceptible to a remote code execution vulnerability. If exploited, this vulnerability would allow an authenticated user to abuse the service, resulting in remote code execution. SolarWinds advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	SolarWinds ARM 2024.3 and prior versions
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.solarwinds.com/trust-center/security-advisories/cve-2024-28991

Affected Product	**HPE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-42772, CVE-2024-21829, CVE-2024-21871, CVE-2024-21781, CVE-2023-43753, CVE-2024-42503, CVE-2024-42502, CVE-2024-42501, CVE-2024-24968, CVE-2024-23984)
Description	HPE has released security updates addressing Multiple Vulnerabilities that exist in their products. If exploited these vulnerabilities could allow an attacker to cause Denial of Service, Information Disclosure, Privilege Escalation. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf04699en_us&docLocale=en_US • https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04709en_us&docLocale=en_US • https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf04705en_us&docLocale=en_US • https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf04706en_us&docLocale=en_US

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-7207, CVE-2024-23651, CVE-2024-23653, CVE-2024-23652, CVE-2024-0553, CVE-2023-5981, CVE-2024-26840, CVE-2021-47113, CVE-2021-47131, CVE-2024-26852, CVE-2021-46955, CVE-2024-26862, CVE-2024-0639, CVE-2024-27043, CVE-2022-48631, CVE-2024-23307, CVE-2022-48651, CVE-2024-26816, CVE-2024-26906, CVE-2024-26689, CVE-2021-47041, CVE-2021-47074, CVE-2024-26744, CVE-2024-26458, CVE-2024-26461, CVE-2024-32487, CVE-2020-1730, CVE-2023-6918, CVE-2023-1667, CVE-2023-48795, CVE-2023-6004, CVE-2020-16135, CVE-2019-14889, CVE-2023-2283, CVE-2021-3634, CVE-2024-25062, CVE-2024-28182, CVE-2023-5388, CVE-2024-20952, CVE-2024-20918, CVE-2024-20921, CVE-2024-20919, CVE-2024-20926, CVE-2024-20945, CVE-2024-21094, CVE-2024-21012, CVE-2024-21068, CVE-2024-21011, CVE-2024-21085, CVE-2023-51385, CVE-2024-22365, CVE-2018-6913, CVE-2017-6512, CVE-2018-6798, CVE-2023-31484, CVE-2024-0985, CVE-2023-52425, CVE-2024-0450, CVE-2024-21626, CVE-2023-42465, CVE-2023-1829, CVE-2023-23559, CVE-2024-28085, CVE-2023-4733, CVE-2023-4738, CVE-2023-4781, CVE-2023-5535, CVE-2023-4750, CVE-2023-4752, CVE-2023-46839)
Description	Dell has released security updates addressing multiple vulnerabilities that exist in their products. These security 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	PowerStore 500T PowerStoreT OS - Versions prior to 4.0.0.2-2365061-retail PowerStore 1000T PowerStoreT OS - Versions prior to 4.0.0.2-2365061-retail PowerStore 1200T PowerStoreT OS - Versions prior to 4.0.0.2-2365061-retail PowerStore 3000T PowerStoreT OS - Versions prior to 4.0.0.2-2365061-retail PowerStore 3200T PowerStoreT OS - Versions prior to 4.0.0.2-2365061-retail PowerStore 5000T PowerStoreT OS - Versions prior to 4.0.0.2-2365061-retail PowerStore 5200T PowerStoreT OS - Versions prior to 4.0.0.2-2365061-retail PowerStore 7000T PowerStoreT OS - Versions prior to 4.0.0.2-2365061-retail PowerStore 9000T PowerStoreT OS - Versions prior to 4.0.0.2-2365061-retail PowerStore 9200T PowerStoreT OS - Versions prior to 4.0.0.2-2365061-retail
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000228610/dsa-2024-398-dell-powerstore-family-security-update-for-multiple-vulnerabilities

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-4441, CVE-2022-0854, CVE-2022-20368, CVE-2022-28748, CVE-2022-2964, CVE-2022-48686, CVE-2022-48751, CVE-2022-48769, CVE-2022-48775, CVE-2022-48778, CVE-2022-48786, CVE-2022-48787, CVE-2022-48788, CVE-2022-48789, CVE-2022-48790, CVE-2022-48791, CVE-2022-48798, CVE-2022-48802, CVE-2022-48805, CVE-2022-48811, CVE-2022-48822, CVE-2022-48823, CVE-2022-48824, CVE-2022-48827, CVE-2022-48834, CVE-2022-48835, CVE-2022-48836, CVE-2022-48837, CVE-2022-48838, CVE-2022-48839, CVE-2022-48843, CVE-2022-48851, CVE-2022-48853, CVE-2022-48856, CVE-2022-48857, CVE-2022-48858, CVE-2022-48865, CVE-2022-48872, CVE-2022-48873, CVE-2022-48901, CVE-2022-48905, CVE-2022-48910, CVE-2022-48912, CVE-2022-48917, CVE-2022-48919, CVE-2022-48920, CVE-2022-48925, CVE-2022-48926, CVE-2022-48928, CVE-2022-48930, CVE-2022-48931, CVE-2022-48933, CVE-2022-48934, CVE-2023-1582, CVE-2023-2176, CVE-2023-52708, CVE-2023-52854, CVE-2023-52893, CVE-2023-52901, CVE-2023-52907, CVE-2024-26583, CVE-2024-26584, CVE-2024-26668, CVE-2024-26677, CVE-2024-26800, CVE-2024-26812, CVE-2024-26851, CVE-2024-27011, CVE-2024-35915, CVE-2024-35933, CVE-2024-35965, CVE-2024-36013, CVE-2024-36270, CVE-2024-36286, CVE-2024-38618, CVE-2024-38662, CVE-2024-39489, CVE-2024-40910, CVE-2024-40984, CVE-2024-41009, CVE-2024-41011, CVE-2024-41012, CVE-2024-41016, CVE-2024-41020, CVE-2024-41035, CVE-2024-41062, CVE-2024-41068, CVE-2024-41087, CVE-2024-41097, CVE-2024-41098, CVE-2024-42077, CVE-2024-42082, CVE-2024-42090, CVE-2024-42101, CVE-2024-42106, CVE-2024-42110, CVE-2024-42148, CVE-2024-42155, CVE-2024-42157, CVE-2024-42158, CVE-2024-42162, CVE-2024-42226, CVE-2024-42228, CVE-2024-42232, CVE-2024-42236, CVE-2024-42240, CVE-2024-42244, CVE-2024-42246, CVE-2024-42259, CVE-2024-42271, CVE-2024-42280, CVE-2024-42281, CVE-2024-42284, CVE-2024-42285, CVE-2024-42286, CVE-2024-42287, CVE-2024-42288, CVE-2024-42289, CVE-2024-42301, CVE-2024-42309, CVE-2024-42310, CVE-2024-42312, CVE-2024-42322, CVE-2024-43819, CVE-2024-43831, CVE-2024-43839, CVE-2024-43853, CVE-2024-43854, CVE-2024-43856, CVE-2024-43861, CVE-2024-43863, CVE-2024-43866, CVE-2024-43871, CVE-2024-43872, CVE-2024-43879, CVE-2024-43882, CVE-2024-43883, CVE-2024-43892, CVE-2024-43893, CVE-2024-43900, CVE-2024-43902, CVE-2024-43905, CVE-2024-43907)
Description	SUSE has released security updates addressing Multiple Vulnerabilities that exist in their products. If exploited this vulnerability could allow an attacker to cause Use After Free, Null Pointer Dereference, Out of Bounds Write. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	OpenSUSE Leap 15.3 SUSE Enterprise Storage 7.1 SUSE Manager Proxy 4.2 SUSE Manager Server 4.2 SUSE Linux Enterprise High Availability Extension 12 SP5, 15 SP3 SUSE Linux Enterprise High Performance Computing 12 SP5, 15 SP3 SUSE Linux Enterprise High Performance Computing LTSS 15 SP3 SUSE Linux Enterprise Live Patching 12-SP5, 15-SP3 SUSE Linux Enterprise Micro 5.1, 5.2 SUSE Linux Enterprise Micro for Rancher 5.2 SUSE Linux Enterprise Server 12 SP5, 15 SP3 SUSE Linux Enterprise Server 15 SP3 Business Critical Linux 15-SP3 SUSE Linux Enterprise Server 15 SP3 LTSS 15-SP3 SUSE Linux Enterprise Server for SAP Applications 12 SP5, 15 SP3 SUSE Linux Enterprise Software Development Kit 12 SP5 SUSE Linux Enterprise Workstation Extension 12 12-SP5 SUSE Manager Retail Branch Server 4.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2024/suse-su-20243249-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20243251-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20243252-1

Affected Product	**F5**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-31484, CVE-2017-10989, CVE-2020-13630)
Description	F5 has released security updates addressing Multiple Vulnerabilities that exist in their products. **CVE-2023-31484 -** CPAN.pm before 2.35 does not verify TLS certificates when downloading distributions over HTTPS. **CVE-2017-10989 -** The getNodeSize function in ext/rtree/rtree.c in SQLite through 3.19.3, as used in GDAL and other products, mishandles undersized RTree blobs in a crafted database, leading to a heap-based buffer over-read or possibly unspecified other impact. **CVE-2020-13630 -** ext/fts3/fts3.c in SQLite before 3.32.0 has a use-after-free in fts3EvalNextRow, related to the snippet feature. F5 advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	F5 Traffix SDC 5.1.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://my.f5.com/manage/s/article/K000141052

Affected Product	**IBM**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-26159, CVE-2022-40023, CVE-2022-25883, CVE-2024-35153, CVE-2023-50312, CVE-2023-45857, CVE-2024-29041, CVE-2023-44270, CVE-2024-4067, CVE-2024-4068, CVE-2024-29415, CVE-2024-28863, CVE-2023-38552, CVE-2023-39333, CVE-2023-45143, CVE-2024-33883)
Description	IBM has released security updates addressing Multiple Vulnerabilities that exist in their products. If exploited these vulnerabilities could allow an attacker to cause Denial of Service, Information Disclosure, Cross-site Scripting. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Offenses Forwarder - Versions 1.0.0 - 1.1.0 InfoSphere Master Data Managemen - Versions 14.0, 12.0, 11.6 IBM Storage Scale System - Versions 6.1.9.2 or earlier Analyst Workflow - Versions 1.0.0 - 2.33.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7168405 • https://www.ibm.com/support/pages/node/7158916 • https://www.ibm.com/support/pages/node/7168573 • https://www.ibm.com/support/pages/node/7168686

Affected Product	**Ubuntu**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities
Description	Ubuntu has released security updates addressing multiple vulnerabilities that exist in Ubuntu Linux kernel. These vulnerabilities could be exploited by malicious users to compromise the affected system. Ubuntu advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ubuntu 24.04 LTS Ubuntu 20.04 LTS Ubuntu 22.04 LTS
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://ubuntu.com/security/notices/USN-7005-1 • https://ubuntu.com/security/notices/USN-7003-3 • https://ubuntu.com/security/notices/USN-7007-1 • https://ubuntu.com/security/notices/USN-7008-1 • https://ubuntu.com/security/notices/USN-7005-2

Affected Product	**Cisco**
Severity	**Medium**
Affected Vulnerability	Command Injection Vulnerability (CVE-2024-20399)
Description	Cisco has released security updates addressing a Command Injection Vulnerability that exists in their products. **CVE-2024-20399 -** A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated user in possession of Administrator credentials to execute arbitrary commands as root on the underlying operating system of an affected device. Cisco advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Cisco products running Cisco NX-OS Software: • MDS 9000 Series Multilayer Switches (CSCwj97007) • Nexus 3000 Series Switches (CSCwj97009) • Nexus 5500 Platform Switches (CSCwj97011) • Nexus 5600 Platform Switches (CSCwj97011) • Nexus 6000 Series Switches (CSCwj97011) • Nexus 7000 Series Switches (CSCwj94682) • Nexus 9000 Series Switches in standalone NX-OS mode (CSCwj97009)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP

Affected Product	**Red Hat**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-52880, CVE-2024-26886, CVE-2024-26974, CVE-2024-38559, CVE-2024-38573, CVE-2024-38615, CVE-2024-40984, CVE-2024-41023, CVE-2024-41031, CVE-2024-42241, CVE-2024-42243, CVE-2024-42246)
Description	Red Hat has released security updates addressing multiple vulnerabilities that exist in their products. These security vulnerabilities could be exploited by malicious users to compromise the affected System. Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Red Hat Enterprise Linux for Real Time for x86_64 - 4 years of updates 9.2 x86_64 Red Hat Enterprise Linux for Real Time for NFV for x86_64 - 4 years of updates 9.2 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.2 x86_64 Red Hat Enterprise Linux Server - AUS 9.2 x86_64 Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.2 s390x Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.2 ppc64le Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.2 aarch64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.2 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.2 x86_64 Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 9.2 x86_64 Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 9.2 ppc64le Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 9.2 s390x Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 9.2 aarch64 Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.2 aarch64 Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.2 s390x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2024:6744 • https://access.redhat.com/errata/RHSA-2024:6745

Disclaimer

The information provided are gathered from official service provider's websites and portals. FinCSIRT strongly recommends members to apply security fixes as per the given guidelines, following the organization's patch and change management procedures to protect systems from potential threats.