Advisory Alert

Alert Number: AAA20240605 **Date:** June 6, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Solarwinds	**High**	Multiple Vulnerabilities
Dell	**High**	Multiple Vulnerabilities
HPE	**High**	Multiple Vulnerabilities
IBM	**High**, Medium, Low	Multiple Vulnerabilities
Red Hat	Medium	Multiple Vulnerabilities

Description

Affected Product	**Solarwinds**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-28996, CVE-2024-28999, CVE-2024-29004)
Description	Solarwinds has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2024-28996** - The SolarWinds Platform was determined to be affected by a SWQL Injection Vulnerability. Attack complexity is high for this vulnerability. **CVE-2024-28999** - The SolarWinds Platform was determined to be affected by a Race Condition Vulnerability affecting the web console. **CVE-2024-29004** - The SolarWinds Platform was determined to be affected by a stored cross-site scripting vulnerability affecting the web console. High-privileged user credentials are needed, and user interaction is required to exploit this vulnerability. Solarwinds advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	SolarWinds Platform 2024.1 SR 1 and previous versions
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.solarwinds.com/trust-center/security-advisories/cve-2024-28996 • https://www.solarwinds.com/trust-center/security-advisories/cve-2024-28999 • https://www.solarwinds.com/trust-center/security-advisories/cve-2024-29004

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-2961,CVE-2024-28757,CVE-2024-28182,CVE-2024-28085,CVE-2024-26600,CVE-2024-26461,CVE-2024-26458,CVE-2024-25743,CVE-2024-25742,CVE-2024-24549,CVE-2024-2398,CVE-2024-23672,CVE-2024-21094,CVE-2024-21085,CVE-2024-21068,CVE-2024-21012,CVE-2024-21011,CVE-2024-2004,CVE-2024-0450,CVE-2023-6597,CVE-2023-6536,CVE-2023-6535,CVE-2023-6356,CVE-2023-5388,CVE-2023-52621,CVE-2023-52605,CVE-2023-52597,CVE-2023-52583,CVE-2023-52582,CVE-2023-52576,CVE-2023-52575,CVE-2023-52574,CVE-2023-52569,CVE-2023-52567,CVE-2023-52566,CVE-2023-52564,CVE-2023-52532,CVE-2023-52529,CVE-2023-52528,CVE-2023-52525,CVE-2023-52524,CVE-2023-52523,CVE-2023-52520,CVE-2023-52519,CVE-2023-52517,CVE-2023-52515,CVE-2023-52513,CVE-2023-52511,CVE-2023-52510,CVE-2023-52509,CVE-2023-52508,CVE-2023-52507,CVE-2023-52504,CVE-2023-52502,CVE-2023-52501,CVE-2023-52497,CVE-2023-52492,CVE-2023-52477,CVE-2023-52474,CVE-2023-52470,CVE-2023-52469,CVE-2023-52454,CVE-2023-52450,CVE-2023-52447,CVE-2023-52425,CVE-2023-40551,CVE-2023-40550,CVE-2023-40549,CVE-2023-40548,CVE-2023-40547,CVE-2023-40546,CVE-2023-35827,CVE-2023-28746,CVE-2022-48630,CVE-2022-48629,CVE-2022-48626,CVE-2022-48624,CVE-2022-4744,CVE-2022-28737,CVE-2022-20154,CVE-2021-47108,CVE-2021-47107,CVE-2021-47105,CVE-2021-47104,CVE-2021-47102,CVE-2021-47101,CVE-2021-47100,CVE-2021-47099,CVE-2021-47098,CVE-2021-47097,CVE-2021-47096,CVE-2021-47095,CVE-2021-47094,CVE-2021-47093,CVE-2021-47091,CVE-2021-47087,CVE-2021-47082,CVE-2021-46936,CVE-2021-46933,CVE-2021-46931,CVE-2021-46930,CVE-2021-46929,CVE-2021-46927,CVE-2021-46926,CVE-2021-46925,CVE-2021-3521)
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	Dell EMC VxRail Appliance 8.0.x versions prior to 8.0.212
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000225710/dsa-2024-244-security-update-for-dell-vxrail-8-0-212-multiple-third-party-component-vulnerabilities

Affected Product	**HPE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-45745, CVE-2023-47855)
Description	HPE has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be locally exploited to allow escalation of privilege and input validation vulnerability. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	HPE Alletra 4110 - Prior to v2.20_05-27-2024 HPE Alletra 4120 - Prior to v2.20_05-27-2024 HPE ProLiant DL110 Gen11 - Prior to v2.20_05-27-2024 HPE ProLiant DL320 Gen11 Server - Prior to v2.20_05-27-2024 HPE ProLiant DL360 Gen11 Server - Prior to v2.20_05-27-2024 HPE ProLiant DL380 Gen11 Server - Prior to v2.20_05-27-2024 HPE ProLiant DL380a Gen11 - Prior to v2.20_05-27-2024 HPE ProLiant DL560 Gen11 - Prior to v2.20_05-27-2024 HPE ProLiant ML110 Gen11 - Prior to v2.20_05-27-2024 HPE ProLiant ML350 Gen11 Server - Prior to v2.20_05-27-2024 HPE Compute Edge Server e930t - Prior to v2.20_05-27-2024
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf04642en_us&docLocale=en_US

Affected Product	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-29025, CVE-2024-22262, CVE-2023-6129, CVE-2024-0727, CVE-2024-22201, CVE-2023-6237)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited to cause Denial of service and Phishing attacks. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM MaaS360 Mobile Enterprise Gateway (MEG) 3.000.400 and prior IBM MaaS360 VPN 3.000.400 and prior
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7156292

Affected Product	**Red Hat**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-4503, CVE-2023-6236, CVE-2024-1102, CVE-2024-1233, CVE-2019-25162, CVE-2020-36777, CVE-2021-46934, CVE-2021-47013, CVE-2021-47055, CVE-2021-47118, CVE-2021-47153, CVE-2021-47171, CVE-2021-47185, CVE-2022-48627, CVE-2022-48669, CVE-2023-6240, CVE-2023-52439, CVE-2023-52445, CVE-2023-52477, CVE-2023-52513, CVE-2023-52520, CVE-2023-52528, CVE-2023-52565, CVE-2023-52578, CVE-τρέχει-52594, CVE-2023-52595, CVE-2023-52598, CVE-2023-52606, CVE-2023-52607, CVE-2023-52610, CVE-2024-0340, CVE-2024-23307, CVE-2024-25744, CVE-2024-26593, CVE-2024-26603, CVE-2024-26610, CVE-2024-26615, CVE-2024-26642, CVE-2024-26643, CVE-2024-26659, CVE-2024-26664, CVE-2024-26693, CVE-2024-26694, CVE-2024-26735, CVE-2024-26743, CVE-2024-26744, CVE-2024-26779, CVE-2024-26872, CVE-2024-26892, CVE-2024-26897, CVE-2024-26901, CVE-2024-26919, CVE-2024-26933, CVE-2024-26934, CVE-2024-26964, CVE-2024-26973, CVE-2024-26993, CVE-2024-27014, CVE-2024-27048, CVE-2024-27052, CVE-2024-27056, CVE-2024-27059)
Description	Red hat has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities may lead to Information disclosure, Integer overflow, Memory corruption, Use-after-free conditions. Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	JBoss Enterprise Application Platform 8.0 for RHEL 8 x86_64 and RHEL 9 x86_64 JBoss Enterprise Application Platform Text-Only Advisories x86_64 Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 9.4 aarch64 Red Hat CodeReady Linux Builder for ARM 64 8 aarch64 and ARM 64 9 aarch64 Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 9.4 s390x Red Hat CodeReady Linux Builder for IBM z Systems 9 s390x Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 9.4 ppc64le Red Hat CodeReady Linux Builder for Power, little endian 8 ppc64le and little endian 9 ppc64le Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 9.4 x86_64 Red Hat CodeReady Linux Builder for x86_64 8 x86_64 and 9 x86_64 Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.4 aarch64 Red Hat Enterprise Linux for ARM 64 8 aarch64 and ARM 64 9 aarch64 Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.4 s390x Red Hat Enterprise Linux for IBM z Systems 8 s390x and IBM z Systems 9 s390x Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.4 ppc64le Red Hat Enterprise Linux for Power, little endian 8 ppc64le and little endian 9 ppc64le Red Hat Enterprise Linux for Real Time 9 x86_64 Red Hat Enterprise Linux for Real Time for NFV 9 x86_64 Red Hat Enterprise Linux for Real Time for NFV for x86_64 - 4 years of updates 9.4 x86_64 Red Hat Enterprise Linux for Real Time for x86_64 - 4 years of updates 9.4 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.4 x86_64 Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.4 x86_64 Red Hat Enterprise Linux for x86_64 8 x86_64 and x86_64 9 x86_64 Red Hat Enterprise Linux Server - AUS 9.4 x86_64 Red Hat Enterprise Linux Server for ARM 64 - 4 years of updates 9.4 aarch64 Red Hat Enterprise Linux Server for IBM z Systems - 4 years of updates 9.4 s390x Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.4 ppc64le
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2024:3580 • https://access.redhat.com/errata/RHSA-2024:3581 • https://access.redhat.com/errata/RHSA-2024:3583 • https://access.redhat.com/errata/RHSA-2024:3618 • https://access.redhat.com/errata/RHSA-2024:3619

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.