Advisory Alert

Alert Number: AAA20240425 **Date:** April 25, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

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

Description

Affected Product	**Juniper**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-35116, CVE-2023-34453, CVE-2023-34455, CVE-2023-34454, CVE-2023-43642, CVE-2023-2976, CVE-2023-33201, CVE-2023-46136, CVE-2023-43804, CVE-2023-37920, CVE-2022-25883, CVE-2023-45133, CVE-2023-31484, CVE-2023-1370, CVE-2021-4048, CVE-2021-23445, CVE-2021-31684, CVE-2023-38019, CVE-2023-38020, CVE-2023-38263, CVE-2023-46308, CVE-2023-32006, CVE-2023-32002, CVE-2023-32559, CVE-2022-38900, CVE-2023-45857, CVE-2022-25927, CVE-2023-44270, CVE-2023-26159, CVE-2020-19909, CVE-2023-38546, CVE-2023-38545, CVE-2023-4807, CVE-2023-0727, CVE-2023-6129, CVE-2023-5363, CVE-2022-21216, CVE-2023-46234)
Description	Juniper has issued security updates addressing multiple vulnerabilities that exist in Juniper Networks Juniper Secure Analytics Applications. If Exploited, these vulnerabilities could lead to Denial of Service, Remote Code Execution, Disclosure of Information. Juniper advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Juniper Networks Juniper Secure Analytics: • Log Collector Application prior to version v1.8.4 • SOAR Plugin Application prior to version 5.3.1 • Deployment Intelligence Application prior to 3.0.12 • User Behavior Analytics Application add-on prior to 4.1.14 • Pulse Application add-on prior to 2.2.12 • Assistant Application add-on prior to 3.6.0 • Use Case Manager Application add-on prior to 3.9.0 • WinCollect Standalone Agent prior to 10.1.8 • M7 Appliances prior to 4.0.0
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-in-JSA-Applications?language=en_US

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-32460, CVE-2023-23583, 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, CVE-2023-20592, CVE-2024-0172, CVE-2023-20593, CVE-2023-31085, CVE-2023-39189, CVE-2023-39192, CVE-2023-39193, CVE-2023-39194, CVE-2023-42754, CVE-2023-45862, CVE-2023-45871, CVE-2023-5717, CVE-2024-20294, CVE-2024-20291, CVE-2024-20267, CVE-2022-41742, CVE-2022-41741, CVE-2021-3618, CVE-2017-20005, CVE-2021-23017, CVE-2019-20372, CVE-2018-16845, CVE-2017-7529, CVE-2016-1247, CVE-2016-4450, CVE-2016-0747, CVE-2016-0746, CVE-2016-0742, CVE-2024-22252, CVE-2024-22253, CVE-2024-22254, CVE-2024-22255, CVE-2023-0673)
Description	Dell has released security updates addressing multiple vulnerabilities that exist in third-party components, consequently impacting Dell PowerFlex 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	PowerFlex Appliance - IC versions prior to IC-38.366.00 PowerFlex Rack- RCM versions prior to 3.6.6.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000224466/dsa-2024-195-security-update-for-dell-powerflex-appliance-multiple-third-party-component-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000224465/dsa-2024-194-security-update-for-dell-powerflex-rack-multiple-third-party-component-vulnerabilities

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-52340, CVE-2024-26622, CVE-2023-5717, CVE-2024-1086)
Description	SUSE has released security updates addressing multiple vulnerabilities that exist in their products. . If Exploited, these vulnerabilities could lead to Denial of Service, Local Privilege Escalation, Heap out-of-bounds write and Use-after-free conditions. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	openSUSE Leap 15.4 SUSE Linux Enterprise High Performance Computing 15 SP4 SUSE Linux Enterprise Live Patching 15-SP4 SUSE Linux Enterprise Micro 5.3, 5.4 SUSE Linux Enterprise Real Time 15 SP4 SUSE Linux Enterprise Server 15 SP4 SUSE Linux Enterprise Server for SAP Applications 15 SP4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2024/suse-su-20241411-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20241418-1/

Affected Product	**Cisco**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-20358, CVE-2024-20353, CVE-2024-20359)
Description	Cisco has released security updates addressing multiple vulnerabilities that exist in Cisco Adaptive Security Appliance and Firepower Threat Defense Software. **CVE-2024-20358-** A Command Injection Vulnerability due to the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. **CVE-2024-20353-** A denial of service vulnerability due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. **CVE-2024-20359-** Local Code Execution Vulnerability due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device Cisco advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Cisco products running on vulnerable release of Cisco Adaptive Security Appliance Software or Firepower Threat Defense Software
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2 • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm

Affected Product	**IBM**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-25710, CVE-2024-26308, CVE-2024-25026, CVE-2024-22354)
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 and XML External Entity (XXE) injection. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Storage Insights - Data Collector version 20240303-0731 IBM WebSphere Application Server 8.5, 9.0 IBM WebSphere Application Server Liberty versions 17.0.0.3 - 24.0.0.4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7149302 • https://www.ibm.com/support/pages/node/7149330 • https://www.ibm.com/support/pages/node/7148426

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.