Advisory Alert

Alert Number: AAA20241121 **Date:** November 21, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Juniper	**Critical**	Multiple vulnerabilities
Dell	**Critical**	Multiple Vulnerabilities
IBM	**Critical**	Nesting-based mXSS Vulnerability
Dell	**High**	Multiple Vulnerabilities
IBM	**High**, Medium	Multiple Vulnerabilities
Drupal	**High**, Medium, Low	Multiple Vulnerabilities

Description

Affected Product	**Juniper**
Severity	Critical - Initial release date **8th February 2024 (AAA20240208)**
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, CVE2021-23445, 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-2023-5678, CVE-2023-46218, CVE-2023-46219, CVE-2023-4807, CVE-2023-0727, CVE2023-6129, CVE-2023-5363, CVE-2022-21216, CVE-2023-46234, CVE-2024-28849, CVE-2024-29041, CVE-2024-29180, CVE-2024-4067, CVE-2024-4068, CVE-2024-21501, CVE-2024-27088, CVE-2024-27982, CVE-2024-27983, CVE-2021-23727, CVE-2024-39338, CVE-2019-13224, CVE-2019-16163, CVE-2019-19012, CVE-2022-24735, CVE-2022-24736, CVE-2022-24834, CVE-2023-28856, CVE-2023-45145)
Description	Juniper has released security updates addressing multiple vulnerabilities that exist in Juniper Secure Analytics optional Applications. These vulnerabilities could be exploited by malicious users to cause Denial of Service, Fatal Errors, Directory traversal, Information Disclosure, Authentication Bypass. 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 3.0.14 • User Behavior Analytics Application add-on prior to 4.1.14 • Pulse Application add-on prior to 2.2.14 • Assistant Application add-on prior to 3.8.0 • 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 • Log Source Management App prior to 7.0.8
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://supportportal.juniper.net/s/article/On-Demand-JSA-Series-Multiple-vulnerabilities-resolved-in-JSA-Applications?language=en_US

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-38304, CVE-2024-38303, CVE-2024-24852, CVE-2024-36274, CVE-2024-24853, CVE-2024-21781, CVE-2024-21810. CVE-2024-24983, CVE-2024-23497, CVE-2024-21769, CVE-2024-23981, CVE-2024-24986, CVE-2024-23499, CVE-2024-21807, CVE-2024-21806, CVE-2024-22376, CVE-2024-6387, CVE-2024-38433, CVE-2024-37086, CVE-2024-37087, CVE-2024-37081, CVE-2024-37080, CVE-2024-37079, CVE-2024-22275, CVE-2024-22274, CVE-2024-22273, CVE-2024-33600, CVE-2024-33599, CVE-2024-2961, CVE-2017-9271, CVE-2024-33601, CVE-2024-38428)
Description	Dell has released security updates addressing multiple vulnerabilities that exist in third party products which affect PowerProtect Data Manager Software. 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	PowerProtect Data Manager DM5500 Appliance Versions 5.14.0.0 through 5.17.0.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000250694/dsa-2024-458-security-update-for-dell-powerprotect-data-manager-appliance-dm5500-multiple-third-party-component-vulnerabilities

Affected Product	**IBM**
Severity	**Critical**
Affected Vulnerability	Nesting-based mXSS Vulnerability (CVE-2024-47875)
Description	IBM has released security updates addressing a Nesting-based mXSS Vulnerability that exists in a third party product which affects QRadar User Behavior Analytics. **CVE-2024-47875** - DOMPurify is a DOM-only, super-fast, uber-tolerant XSS sanitizer for HTML, MathML and SVG. DOMpurify was vulnerable to nesting-based mXSS. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	QRadar User Behavior Analytics versions 1.0.0 - 4.1.16
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7176642

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-5363, CVE-2023-5678, CVE-2023-6237, CVE-2024-0727, CVE-2024-21844, CVE-2023-34424, CVE-2023-35061, CVE-2023-38655, CVE-2023-40067, CVE-2023-48361, CVE-2024-24853, CVE-2024-24980, CVE-2023-22351, CVE-2023-23904, CVE-2023-25546, CVE-2023-34440, CVE-2023-41833, CVE-2023-43753, CVE-2023-43758, CVE-2024-21781, CVE-2024-21829, CVE-2024-21871, CVE-2024-23599, CVE-2024-24968, CVE-2024-23984, CVE-2024-5462, CVE-2020-24977, CVE-2021-3517, CVE-2021-3518, CVE-2021-3537, CVE-2021-3541, CVE-2022-40304, CVE-2023-28484, CVE-2023-29469)
Description	Dell has released security updates addressing multiple vulnerabilities that exist in third party products which 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	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000226215/dsa-2024-281-security-update-for-dell-client-platform-for-multiple-openssl-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000225475/dsa-2024-243-security-update-for-dell-client-platform-for-intel-platform-update-2024-3-advisories • https://www.dell.com/support/kbdoc/en-us/000228212/dsa-2024-358-security-update-for-dell-connectrix-brocade-for-multiple-third-party-component-vulnerabilities

Affected Product	**IBM**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2019-8331, CVE-2018-20676, CVE-2018-20677, CVE-2018-14040, CVE-2018-14041, CVE-2016-10735, CVE-2024-39338, CVE-2024-5569, CVE-2024-45801, CVE-2024-1135, CVE-2024-39689, CVE-2024-34064, CVE-2024-47831, CVE-2024-6345, CVE-2024-43788, CVE-2024-4068, CVE-2024-34069, CVE-2024-37891, CVE-2024-34351, CVE-2024-39338, CVE-2024-47831, CVE-2024-46982, CVE-2023-26159, CVE-2024-28849, CVE-2024-45296, CVE-2024-43800, CVE-2024-43799, CVE-2024-43796, CVE-2024-45590, CVE-2024-45663)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Cross-Site Scripting, Server-Side Request Forgery, Denial of Service, Arbitrary Code Execution. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	QRadar User Behavior Analytics versions 1.0.0 - 4.1.16 IBM QRadar Pre-Validation App versions 1.0.0 - 2.0.0 IBM QRadar Pulse App versions 1.0.0 - 2.2.14 IBM Db2 Server versions 11.1.4 - 11.1.4.7, 11.5.0 - 11.5.9 and 12.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7176642 • https://www.ibm.com/support/pages/node/7176657 • https://www.ibm.com/support/pages/node/7176660 • https://www.ibm.com/support/pages/node/7175943

Affected Product	**Drupal**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities
Description	Drupal has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Arbitrary PHP code execution, PHP Object Injection, cross-site scripting and Access bypass. Drupal advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Drupal core for Drupal 7 versions prior to 7.102 Drupal core for Drupal 10.2 versions prior to 10.2.11 Drupal core for Drupal 10.3 versions prior to 10.3.9 Drupal core for Drupal 11.0 versions prior to 11.0.8 Node export versions prior to 7.x-3.3 Mailjet module version prior to 4.0.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.drupal.org/sa-contrib-2024-062 • https://www.drupal.org/sa-core-2024-008 • https://www.drupal.org/sa-core-2024-007 • https://www.drupal.org/sa-core-2024-006 • https://www.drupal.org/sa-core-2024-005 • https://www.drupal.org/sa-core-2024-004 • https://www.drupal.org/sa-core-2024-003 • https://www.drupal.org/sa-contrib-2024-061

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.