Advisory Alert

Alert Number: AAA20230621 **Date:** June 21, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Ivanti	**Critical**	Remote Code Execution Vulnerability
Ivanti	**High**	Multiple Vulnerabilities
Suse	**High**	Multiple Vulnerabilities
Dell	**High**	Multiple Vulnerabilities
NodeJS	**High**, Medium	Multiple Vulnerabilities
IBM	**High**, Medium, Low	Multiple Vulnerabilities

Description

Affected Product	**Ivanti**
Severity	**Critical**
Affected Vulnerability	Remote Code Execution Vulnerability (CVE-2023-28323)
Description	Ivanti has released a security update addressing a Remote Code Execution vulnerability that exists in Ivanti Endpoint Manager. The vulnerability could allow an unauthenticated user to elevate privileges and migrate to other network attached machines. Ivanti highly recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	EPM 2022 SU3 and all previous versions.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://forums.ivanti.com/s/article/SA-2023-06-20-CVE-2023-28323?language=en_US

Affected Product	**Ivanti**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-28324)
Description	Ivanti has released a security update addressing a Privilege Escalation vulnerability and Remote Code Execution vulnerability that exists in Ivanti Endpoint Manager. The vulnerability could allow an unauthenticated user to elevate rights. Ivanti highly recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Endpoint Manager 2022, Endpoint Manager 2020.1, Endpoint Manager 2021.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://forums.ivanti.com/s/article/SA-2023-06-06-CVE-2023-28324?language=en_US

Affected Product	**Suse**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-3566, CVE-2022-45884, CVE-2022-45885, CVE-2022-45886, CVE-2022-45887, CVE-2022-45919, CVE-2023-1077, CVE-2023-1380, CVE-2023-2176, CVE-2023-2194, CVE-2023-2483, CVE-2023-2513, CVE-2023-28466, CVE-2023-31084, CVE-2023-31436, CVE-2023-32269, CVE-2023-2269)
Description	Suse has released security updates addressing multiple vulnerabilities in their products. If exploited these vulnerabilities could cause use-after-free condition, out-of-bounds write, out-of-bounds read and Denial of Service. Suse recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	openSUSE Leap 15.4, 15.5 SUSE CaaS Platform 4.0 SUSE Linux Enterprise High Availability Extension 12 SP4, 12 SP5, 15 SP1 SUSE Linux Enterprise High Performance Computing 12 SP4, 12 SP5, 15 SP1, 15 SP1 LTSS 15-SP1 SUSE Linux Enterprise Live Patching 12-SP4, 12-SP5, 15-SP1 SUSE Linux Enterprise Server 12 SP4, 12 SP4 ESPOS 12-SP4, 12 SP4 LTSS 12-SP4, 12 SP5 SUSE Linux Enterprise Server 15 SP1 SUSE Linux Enterprise Server 15 SP1 Business Critical Linux 15-SP1 SUSE Linux Enterprise Server 15 SP1 LTSS 15-SP1 SUSE Linux Enterprise Server for SAP Applications 12 SP4, 12 SP5, 15 SP1 SUSE Linux Enterprise Software Development Kit 12 SP5 SUSE Linux Enterprise Workstation Extension 12 12-SP5 SUSE Manager Proxy 4.0 SUSE Manager Retail Branch Server 4.0 SUSE Manager Server 4.0 SUSE OpenStack Cloud 9 SUSE OpenStack Cloud Crowbar 9
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2023/suse-su-20232534-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20232537-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20232538-1/

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-33117, CVE-2021-0154, CVE-2021-0153, CVE-2021-33123, CVE-2021-0190, CVE-2021-33122, CVE-2021-0189, CVE-2021-33124, CVE-2021-33103, CVE-2021-0159, CVE-2021-0188, CVE-2021-0155, CVE-2022-0004, CVE-2022-0005, CVE-2022-21131, CVE-2022-21136, CVE-2022-21127, CVE-2022-21125, CVE-2022-21166, CVE-2022-34377, CVE-2022-34376, CVE-2022-34406, CVE-2022-34407, CVE-2022-34408, CVE-2022-34409, CVE-2022-34410, CVE-2022-34411, CVE-2022-34412, CVE-2022-34413, CVE-2022-34414, CVE-2022-34415, CVE-2022-34416, CVE-2022-34417, CVE-2022-34418, CVE-2022-34419, CVE-2022-34420, CVE-2022-34421, CVE-2022-34422, CVE-2022-34423)
Description	Dell has released a security update addressing multiple vulnerabilities that exist in their products. Exploitation of the vulnerabilities could cause Information disclosure, Privilege escalation, Denial of Service, Arbitrary Code execution. Dell recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Disk Library for mainframe DLm8500 Disk Library for mainframe DLm2500
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000215126/dsa-2023-151-security-update-for-dell-emc-dlm

Affected Product	**NodeJS**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-30581, CVE-2023-30584, CVE-2023-30582, CVE-2023-30583, CVE-2023-30585, CVE-2023-30586, CVE-2023-30588, CVE-2023-30589, CVE-2023-30590)
Description	NodeJS has released a security update addressing multiple vulnerabilities that exist in their products. Exploitation of the vulnerabilities could cause Path traversal bypass, Privilege escalation, Smuggling of HTTP Requests and Process interruption NodeJS recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	All versions of the 20.x, 18.x, and 16.x release lines.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://nodejs.org/en/blog/vulnerability/june-2023-security-releases

Affected Product	**IBM**
Severity	**High** , **Medium** , **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-29257, CVE-2023-29255, CVE-2023-27555, CVE-2023-26021, CVE-2023-25930, CVE-2023-26022, CVE-2023-27559, CVE-2022-43929, CVE-2022-43927, CVE-2014-3577, CVE-2022-43930, CVE-2022-25647, CVE-2022-31159, CVE-2023-28956, CVE-2022-41723, CVE-2023-26283, CVE-2023-24998)
Description	IBM has released security updates addressing Multiple Vulnerabilities in their products. If exploited theses vulnerabilities could lead to denial of service, information disclosure and Privilege Escalation. IBM recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	IBM dashDB Local IBM Storage Protect Server Versions 8.1.0.000 - 8.1.18.xxx IBM Spectrum Protect Backup-Archive Client8.1.0.0 - 8.1.17.2 IBM Operations Analytics Predictive Insights 1.3.5 IBM Operations Analytics Predictive Insights 1.3.6’ Websphere Application Server 9.0 IBM Robotic Process Automation 21.0.0 - 21.0.7.5 IBM Robotic Process Automation 23.0.0 - 23.0.5 IBM Robotic Process Automation for Cloud Pak 21.0.0 - 21.0.7.5 IBM Robotic Process Automation for Cloud Pak 23.0.0 - 23.0.5 IBM WebSphere Application Server Patterns1.0.0.0 - 1.0.0.7 IBM WebSphere Application Server Patterns2.2.0.0 - 2.3.3.6
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7005553 https://www.ibm.com/support/pages/node/7005605 https://www.ibm.com/support/pages/node/7005577 https://www.ibm.com/support/pages/node/7005519 https://www.ibm.com/support/pages/node/7005569 https://www.ibm.com/support/pages/node/7005489 https://www.ibm.com/support/pages/node/7005549 https://www.ibm.com/support/pages/node/7005623

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.