# Advisory Alert

**Alert Number:** AAA20240513 **Date:** May 13, 2024

**Document Classification Level** : Public Circulation Permitted | Public

**Information Classification Level** : TLP: WHITE

## Overview

| Product | Severity | Vulnerability |
|---|---|---|
| **IBM** | **Critical** | Multiple Vulnerabilities |
| **Dell** | **High** | Insecure Deserialization Vulnerability |
| **SUSE** | **High** | Multiple Vulnerabilities |
| **Lenovo** | **High** | Multiple Vulnerabilities |
| **IBM** | **High**, **Medium**, **Low** | Multiple Vulnerabilities |

## Description

| | |
|---|---|
| Affected Product | **IBM** |
| Severity | **Critical** |
| Affected Vulnerability | Multiple Vulnerabilities (CVE-2023-41419, CVE-2020-13936) |
| Description | IBM has issued security updates addressing multiple vulnerabilities that exist in IBM QRadar User Behavior Analytics.<br>**CVE-2023-41419** - Gevent could allow a remote attacker to gain elevated privileges on the system, caused by a flaw in the WSGIServer component. By using a specially crafted script, an attacker could exploit this vulnerability to gain elevated privileges.<br>**CVE-2020-13936** - Apache Velocity could allow a remote attacker to execute arbitrary code on the system, caused by a sandbox bypass flaw. By modifying the Velocity templates, an attacker could exploit this vulnerability to execute arbitrary code with the same privileges as the account running the Servlet container.<br>IBM advises to apply security fixes at your earliest to protect systems from potential threats. |
| Affected Products | IBM QRadar User Behavior Analytics 1.0.0 - 4.1.15 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://www.ibm.com/support/pages/node/7150844 |

| | |
|---|---|
| Affected Product | **Dell** |
| Severity | **High** |
| Affected Vulnerability | Insecure Deserialization Vulnerability (CVE-2024-28964) |
| Description | Dell has released security updates addressing an Insecure Deserialization Vulnerability that exists in Dell EMC Common Event Enabler. A local unauthenticated attacker could potentially exploit this vulnerability, leading to arbitrary code execution in the context of the logged in user. Exploitation of this issue requires a victim to open a malicious file.<br>Dell advises to apply security fixes at your earliest to protect systems from potential threats. |
| Affected Products | Dell EMC Common Event Enabler, CAVATools for Windows - Versions prior to 8.9.10.0 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://www.dell.com/support/kbdoc/en-us/000224987/dsa-2024-179-security-update-for-dell-emc-common-event-enabler-windows-for-cavatools-vulnerabilities |

| | |
|---|---|
| Affected Product | **SUSE** |
| Severity | **High** |
| Affected Vulnerability | Multiple Vulnerabilities (CVE-2024-0775, CVE-2024-1086, CVE-2024-26622, CVE-2023-5717) |
| Description | SUSE has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Heap Out-Of-Bounds Writes and Use-After-Free Conditions.<br>SUSE advises to apply security fixes at your earliest to protect systems from potential threats. |
| Affected Products | openSUSE Leap 15.3, 15.4, 15.5<br>SUSE Linux Enterprise High Performance Computing 15 SP3, 15 SP4, 15 SP5<br>SUSE Linux Enterprise Live Patching 15 SP3, 15 SP4, 15 SP5<br>SUSE Linux Enterprise Micro 5.1, 5.2, 5.3, 5.4, 5.5<br>SUSE Linux Enterprise Real Time 15 SP4, 15 SP5<br>SUSE Linux Enterprise Server 15 SP3, 15 SP4, 15 SP5<br>SUSE Linux Enterprise Server for SAP Applications 15 SP3, 15 SP4, 15 SP5 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | • https://www.suse.com/support/update/announcement/2024/suse-su-20241596-1/<br>• https://www.suse.com/support/update/announcement/2024/suse-su-20241582-1/ |

| | |
|---|---|
| Affected Product | **Lenovo** |
| Severity | **High** |
| Affected Vulnerability | Multiple Vulnerabilities (CVE-2022-24351, CVE-2022-27879, CVE-2022-37343, CVE-2022-38083, CVE-2022-40982, CVE-2022-41804, CVE-2022-43505, CVE-2022-44611, CVE-2022-46897, CVE-2023-2004, CVE-2023-20555, CVE-2023-20569, CVE-2023-23908, CVE-2023-26090, CVE-2023-27471, CVE-2023-28468, CVE-2023-31041, CVE-2023-34419, CVE-2023-4028, CVE-2023-4029, CVE-2023-4030, CVE-2021-26345, CVE-2021-46758, CVE-2021-46766, CVE-2021-46774, CVE-2022-23820, CVE-2022-23821, CVE-2022-23830, CVE-2023-20519, CVE-2023-20521, CVE-2023-20526, CVE-2023-20533, CVE-2023-20563, CVE-2023-20565, CVE-2023-20566, CVE-2023-20571, CVE-2023-20592, CVE-2023-20596, CVE-2023-22329, CVE-2023-23583, CVE-2023-25756, CVE-2023-30633, CVE-2023-31100, CVE-2023-34195, CVE-2023-5075, CVE-2023-5078, CVE-2023-20594, CVE-2023-20597, CVE-2023-25493, CVE-2023-25494, CVE-2023-43567, CVE-2023-43568, CVE-2023-43569, CVE-2023-43570, CVE-2023-43571, CVE-2023-43572, CVE-2023-43573, CVE-2023-43574, CVE-2023-43575, CVE-2023-43576, CVE-2023-43577, CVE-2023-43578, CVE-2023-43579, CVE-2023-43580, CVE-2023-43581, CVE-2023-45075, CVE-2023-45076, CVE-2023-45077, CVE-2023-45078, CVE-2023-20579, CVE-2023-20587, CVE-2023-25174, CVE-2023-28388, CVE-2023-28739, CVE-2023-29153, CVE-2023-31346, CVE-2023-31347, CVE-2023-34469, CVE-2023-34470, CVE-2023-35841, CVE-2023-45229, CVE-2023-45230, CVE-2023-45231, CVE-2023-45232, CVE-2023-45233, CVE-2023-45234, CVE-2023-45235, CVE-2020-5952, CVE-2022-30426, CVE-2023-22655, CVE-2023-28149, CVE-2023-28746, CVE-2023-32282, CVE-2023-32666, CVE-2023-38575, CVE-2023-39281, CVE-2023-39283, CVE-2023-39284, CVE-2023-39368, CVE-2023-5912) |
| Description | Lenovo has released security updates addressing multiple vulnerabilities that exist their products. Exploitation of these vulnerabilities may lead to Denial of Service, Unauthorized Access, Improper Authorization, Information Disclosure.<br>Lenovo 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.lenovo.com/us/en/product_security/LEN-134879<br>• https://support.lenovo.com/us/en/product_security/LEN-140141<br>• https://support.lenovo.com/us/en/product_security/LEN-141775<br>• https://support.lenovo.com/us/en/product_security/LEN-145284<br>• https://support.lenovo.com/us/en/product_security/LEN-150692<br>• https://support.lenovo.com/us/en/product_security/LEN-155477 |

| | |
|---|---|
| Affected Product | **IBM** |
| Severity | **High**, **Medium**, **Low** |
| Affected Vulnerability | Multiple Vulnerabilities |
| Description | IBM has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Privilege escalation, Directory traversal, Sensitive information disclosure, LDAP injection.<br>IBM advises to apply security fixes at your earliest to protect systems from potential threats. |
| Affected Products | IBM QRadar SIEM 7.5 - 7.5.0 UP8<br>IBM Storage Fusion 2.5.0 - 2.7.2<br>IBM Storage Fusion HCI 2.5.2 - 2.7.2<br>IBM QRadar User Behavior Analytics 1.0.0 - 4.1.15<br>IBM WebSphere Extreme Scale 8.6.1.0 - 8.6.1 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | • https://www.ibm.com/support/pages/node/7150846<br>• https://www.ibm.com/support/pages/node/7150929<br>• https://www.ibm.com/support/pages/node/7151040<br>• https://www.ibm.com/support/pages/node/7151041<br>• https://www.ibm.com/support/pages/node/7151043<br>• https://www.ibm.com/support/pages/node/7151044<br>• https://www.ibm.com/support/pages/node/7151045<br>• https://www.ibm.com/support/pages/node/7151046<br>• https://www.ibm.com/support/pages/node/7151047<br>• https://www.ibm.com/support/pages/node/7151048<br>• https://www.ibm.com/support/pages/node/7151049<br>• https://www.ibm.com/support/pages/node/7151050<br>• https://www.ibm.com/support/pages/node/7151051<br>• https://www.ibm.com/support/pages/node/7151052 |

### 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.**