# Advisory Alert

**Alert Number:** **AAA20240325** **Date:** **March 25, 2024**

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

**Information Classification Level** : TLP: WHITE

**Overview**

| Product | Severity | Vulnerability |
|---|---|---|
| **IBM** | **Critical** | Expression Language Injection Vulnerability |
| **Microsoft** | **High** | Information Disclosure Vulnerability |
| **Hitachi** | **High** | Security Updates |
| **Suse** | **High** | Multiple Vulnerabilities |
| **IBM** | **High**,<br>**Medium**,<br>**Low** | Multiple Vulnerabilities |

**Description**

| | |
|---|---|
| Affected Product | **IBM** |
| Severity | **Critical** |
| Affected Vulnerability | Expression Language Injection Vulnerability (CVE-2022-22980) |
| Description | IBM has issued a security update addressing an Expression Language Injection vulnerability within third-party components that impact IBM Storage Copy Data Management. The vulnerability exists due to SpEL injection issue through annotated repository query methods. A remote attacker can execute arbitrary code on the target system.<br>IBM advises to apply security fixes at your earliest to protect your systems from potential threats. |
| Affected Products | IBM Storage Copy Data Management 2.2.0.0 - 2.2.22.1 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://www.ibm.com/support/pages/node/7123182 |

| | |
|---|---|
| Affected Product | **Microsoft** |
| Severity | **High** |
| Affected Vulnerability | Information Disclosure Vulnerability (CVE-2024-29059) |
| Description | Microsoft has released a security update addressing an Information Disclosure Vulnerability that exists their products. An attacker who successfully exploited this vulnerability could obtain the ObjRef URI which could lead to Remote Code Execution.<br>Microsoft advises to apply security fixes at your earliest to protect your systems from potential threats. |
| Affected Products | Microsoft .NET Framework 3.5.1<br>Microsoft .NET Framework 3.5<br>Microsoft .NET Framework 3.0 Service Pack 2<br>Microsoft .NET Framework 2.0 Service Pack 2<br>Microsoft .NET Framework 3.5 AND 4.6/4.6.2<br>Microsoft .NET Framework 4.6.2<br>Microsoft .NET Framework 3.5 AND 4.8.1<br>Microsoft .NET Framework 4.6.2/4.7/4.7.1/4.7.2<br>Microsoft .NET Framework 3.5 AND 4.6.2/4.7/4.7.1/4.7.2/4.8<br>Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)<br>Windows Server 2008 R2 for x64-based Systems Service Pack 1<br>Windows Server 2012 R2 (Server Core installation)<br>Windows Server 2012 R2<br>Windows Server 2012 (Server Core installation)<br>Windows Server 2012<br>Windows Server 2008 for x64-based Systems Service Pack 2<br>Windows Server 2008 for 32-bit Systems Service Pack 2<br>Windows 10 for x64-based Systems<br>Windows 10 for 32-bit Systems<br>Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)<br>Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)<br>Windows Server 2022, 23H2 Edition (Server Core installation)<br>Windows 11 Version 23H2 for x64-based Systems<br>Windows 11 Version 23H2 for ARM64-based Systems<br>Windows 10 Version 22H2 for 32-bit Systems<br>Windows 10 Version 22H2 for ARM64-based Systems<br>Windows 10 Version 22H2 for x64-based Systems<br>Windows 11 Version 22H2 for x64-based Systems<br>Windows 11 Version 22H2 for ARM64-based Systems<br>Windows 10 Version 21H2 for x64-based Systems<br>Windows 10 Version 21H2 for ARM64-based Systems<br>Windows 10 Version 21H2 for 32-bit Systems<br>Windows 11 version 21H2 for ARM64-based Systems<br>Windows 11 version 21H2 for x64-based Systems<br>Windows Server 2022 (Server Core installation)<br>Windows Server 2022<br>Windows 10 Version 1607 for x64-based Systems<br>Windows 10 Version 1607 for 32-bit Systems<br>Windows Server 2016 (Server Core installation)<br>Windows Server 2016<br>Windows Server 2019 (Server Core installation)<br>Windows Server 2019<br>Windows 10 Version 1809 for ARM64-based Systems<br>Windows 10 Version 1809 for x64-based Systems |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-29059 |

| | |
|---|---|
| Affected Product | **Hitachi** |
| Severity | **High** |
| Affected Vulnerability | Security Updates (CVE-2022-36407) |
| Description | Hitachi has released security updates addressing the plaintext storage of passwords in Hitachi Disk Array Systems.<br>Hitachi recommends to apply security fixes at your earliest to protect your systems from potential threats. |
| Affected Products | Hitachi Unified Storage VM<br>Hitachi Virtual Storage Platform<br>Hitachi Virtual Storage Platform VP9500<br>Hitachi Virtual Storage Platform G1000, G1500<br>Hitachi Virtual Storage Platform F1500<br>Hitachi Virtual Storage Platform 5100, 5500, 5100H, 5500H<br>Hitachi Virtual Storage Platform 5200, 5600, 5200H, 5600H<br>Hitachi Virtual Storage Platform G100, G200, G400, G600, G800<br>Hitachi Virtual Storage Platform F400, F600, F800<br>Hitachi Virtual Storage Platform G130, G150, G350, G370, G700, G900<br>Hitachi Virtual Storage Platform F350, F370, F700, F900<br>Hitachi Virtual Storage Platform E590, E790, E990, E1090, E590H, E790H, E1090H |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://www.hitachi.com/products/it/storage-solutions/sec_info/2024/2022_313.html |

| | |
|---|---|
| Affected Product | **SUSE** |
| Severity | **High** |
| Affected Vulnerability | Multiple Vulnerabilities (CVE-2019-25162, CVE-2021-46923, CVE-2021-46924, CVE-2021-46932, CVE-2021-46934, CVE-2021-47083, CVE-2022-48627, CVE-2023-28746, CVE-2023-5197, CVE-2023-52340, CVE-2023-52429, CVE-2023-52439, CVE-2023-52443, CVE-2023-52445, CVE-2023-52447, CVE-2023-52448, CVE-2023-52449, CVE-2023-52451, CVE-2023-52452, CVE-2023-52456, CVE-2023-52457, CVE-2023-52463, CVE-2023-52464, CVE-2023-52467, CVE-2023-52475, CVE-2023-52478, CVE-2023-52482, CVE-2023-52484, CVE-2023-52530, CVE-2023-52531, CVE-2023-52559, CVE-2023-6270, CVE-2023-6817, CVE-2024-0607, CVE-2024-1151, CVE-2024-23849, CVE-2024-23850, CVE-2024-23851, CVE-2024-26585, CVE-2024-26586, CVE-2024-26589, CVE-2024-26591, CVE-2024-26593, CVE-2024-26595, CVE-2024-26598, CVE-2024-26602, CVE-2024-26603, CVE-2024-26607, CVE-2024-26622, CVE-2020-36777, CVE-2020-36784, CVE-2021-33200, CVE-2021-46906, CVE-2021-46915, CVE-2021-46921, CVE-2021-46929, CVE-2021-46953, CVE-2021-46974, CVE-2021-46991, CVE-2021-46992, CVE-2021-47013, CVE-2021-47054, CVE-2021-47076, CVE-2021-47077, CVE-2021-47078, CVE-2022-20154, CVE-2023-35827, CVE-2023-46343, CVE-2023-52502, CVE-2023-52532, CVE-2023-52574, CVE-2023-52597, CVE-2023-52605, CVE-2023-6356, CVE-2023-6535, CVE-2023-6536, CVE-2024-26600) |
| Description | SUSE has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited to cause Out of bounds read, Infinite loop, NULL pointer dereference, kernel crash.<br>SUSE advises to apply security fixes at your earliest to protect your systems from potential threats. |
| Affected Products | openSUSE Leap Micro 5.3, 5.4<br>SUSE Linux Enterprise High Performance Computing 12 SP5, 12 SP4<br>SUSE Linux Enterprise Live Patching 15-SP4<br>SUSE Linux Enterprise Micro 5.3, 5.4<br>SUSE Linux Enterprise Micro for Rancher 5.3, 5.4<br>SUSE Linux Enterprise Real Time 12 SP5, 15 SP4<br>SUSE Linux Enterprise Server 12 SP5, 15 SP4<br>SUSE Linux Enterprise Server for SAP Applications 12 SP5, 15 SP4 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://www.suse.com/support/update/announcement/2024/suse-su-20240977-1/<br>https://www.suse.com/support/update/announcement/2024/suse-su-20240976-1/<br>https://www.suse.com/support/update/announcement/2024/suse-su-20240975-1/ |

| | |
|---|---|
| Affected Product | **IBM** |
| Severity | **High**, **Medium**, **Low** |
| Affected Vulnerability | Multiple Vulnerabilities (CVE-2023-24998, CVE-2023-28708, CVE-2023-34981, CVE-2022-42252, CVE-2023-28709, CVE-2023-41080, CVE-2022-25762, CVE-2021-43980, CVE-2022-29885, CVE-2021-41079, CVE-2023-42795, CVE-2023-45648, CVE-2024-21733, CVE-2023-51441, CVE-2023-3817, CVE-2023-3446, CVE-2023-4622, CVE-2023-2162, CVE-2023-5678, CVE-2023-5633, CVE-2023-42753, CVE-2021-32036, CVE-2021-32040, CVE-2023-1409, CVE-2023-49083, CVE-2023-46136, CVE-2022-22950, CVE-2022-27772, CVE-2022-22971, CVE-2022-22976, CVE-2022-22978, CVE-2021-22060, CVE-2022-22970) |
| 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, Sensitive information disclosure, Server-side request forgery, Privilege escalation.<br>IBM recommends to apply security fixes at your earliest to protect your systems from potential threats. |
| Affected Products | IBM Storage Copy Data Management 2.2.0.0 - 2.2.22.1<br>IBM Storage Sentinel Anomaly Scan Engine 1.1.0 - 1.1.6 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://www.ibm.com/support/pages/node/7123949<br>https://www.ibm.com/support/pages/node/7123948<br>https://www.ibm.com/support/pages/node/7123184<br>https://www.ibm.com/support/pages/node/7130801<br>https://www.ibm.com/support/pages/node/7123950 |

**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.**