# Advisory Alert

**Alert Number:** AAA20231222 **Date:** December 22, 2023

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

**Information Classification Level :** TLP: WHITE

## Overview

| Product | Severity | Vulnerability |
|---|---|---|
| **HPE** | **Critical** | Multiple Vulnerabilities |
| **SolarWinds** | **High** | Sensitive Data Disclosure Vulnerability |
| **IBM** | **High**, Medium | Multiple Vulnerabilities |

## Description

| | |
|---|---|
| Affected Product | **HPE** |
| Severity | **Critical** |
| Affected Vulnerability | Multiple Vulnerabilities (CVE-2022-24834, CVE-2023-32002, CVE-2023-38552) |
| Description | HPE has released a security update addressing multiple critical vulnerabilities in HPE Unified OSS Console. These vulnerabilities could be exploited to cause Access Restriction Bypass, Arbitrary Code Execution, Authentication Bypass, Compromise of System Integrity and Buffer Overflow.<br>HPE highly recommends to apply the necessary patch updates at your earliest to avoid issues. |
| Affected Products | HPE Unified OSS Console (UOC) - Prior to v3.1.0 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbmu04573en_us |

| | |
|---|---|
| Affected Product | **SolarWinds** |
| Severity | **High** |
| Affected Vulnerability | Sensitive Data Disclosure Vulnerability (CVE-2023-40058) |
| Description | SolarWinds has released a security update addressing a Sensitive Data Disclosure Vulnerability in Access Rights Manager. Sensitive data was added to the public-facing knowledgebase that, if exploited, could be used to access components of Access Rights Manager (ARM) if the threat actor is in the same environment.<br>SolarWinds recommends to apply the necessary patch updates at your earliest to avoid issues. |
| Affected Products | Access Rights Manager (ARM) 2023.2.1 and previous versions |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://www.solarwinds.com/trust-center/security-advisories/cve-2023-40058 |

| | |
|---|---|
| Affected Product | **IBM** |
| Severity | **High**, Medium |
| Affected Vulnerability | Multiple Vulnerabilities (CVE-2022-42003, CVE-2023-35116, CVE-2023-3635, CVE-2022-3172, CVE-2022-3162, CVE-2023-45133, CVE-2022-25883, CVE-2023-44270, CVE-2020-28851, CVE-2020-28852, CVE-2021-44716, CVE-2022-30633, CVE-2022-27664, CVE-2022-28131, CVE-2022-41721, CVE-2021-43565, CVE-2022-27191) |
| Description | IBM has released multiple security updates addressing various vulnerabilities in their products. These vulnerabilities could be exploited to cause Server-side request forgery, Injection, Denial of Service, Regular Expression Denial of Service (ReDoS), Arbitrary Code Execution.<br>IBM recommends to apply the necessary patch updates at your earliest to avoid issues. |
| Affected Products | IBM Storage Fusion HCI v2.1.0 - v2.6.1 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://www.ibm.com/support/pages/node/7101075<br>https://www.ibm.com/support/pages/node/7101076<br>https://www.ibm.com/support/pages/node/7101077<br>https://www.ibm.com/support/pages/node/7101078<br>https://www.ibm.com/support/pages/node/7101082 |

### 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.**