# Advisory Alert

**Alert Number:** AAA20220201 **Date:** February 1, 2022

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

**Information Classification Level :** TLP: WHITE

## Overview

| Product | Severity | Vulnerability |
|---|---|---|
| **Samba** | **Critical** | Multiple Vulnerabilities |
| **Red Hat** | **High** | Multiple Vulnerabilities |

## Description

| | |
|---|---|
| Affected Product | **Samba** |
| Severity | **Critical** |
| Affected Vulnerability | Multiple Vulnerabilities (CVE-2021-44141, CVE-2021-44142, CVE-2022-0336) |
| Description | Samba has issued software updates to address multiple security vulnerabilities that, if successfully exploited, could allow remote attackers to execute arbitrary code with the root privileges on affected installations.<br>• **CVE-2021-44141**: Information leak via symlinks of existence of files or directories outside of the exported share<br>• **CVE-2021-44142**: Out-of-bounds heap read/write vulnerability in VFS module vfs_fruit allows code execution<br>• **CVE-2022-0336**: Samba AD users with permission to write to an account can impersonate arbitrary services |
| Affected Products | All versions of the Samba file server prior to 4.15.5.<br>All versions of Samba prior to 4.13.17<br>Samba 4.0.0 and later |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://www.samba.org/samba/history/security.html<br>https://www.samba.org/samba/security/CVE-2021-44141.html<br>https://www.samba.org/samba/security/CVE-2021-44142.html<br>https://www.samba.org/samba/security/CVE-2022-0336.html |

| | |
|---|---|
| Affected Product | **Red Hat** |
| Severity | **High** |
| Affected Vulnerability | Multiple Vulnerabilities (CVE-2021-4154, CVE-2021-4155, CVE-2022-0185) |
| Description | Red Hat has released security updates to address several vulnerabilities. It is highly recommended to apply necessary fixes provided on the official Red Hat website at the earliest to avoid these security issues, and all Red Hat users are encouraged to upgrade to the latest versions.<br>• **CVE-2021-4154**: kernel - local privilege escalation by exploiting the fsconfig syscall parameter leads to container breakout<br>• **CVE-2021-4155**: kernel - xfs: raw block device data leak in XFS_IOC_ALLOCSP IOCTL<br>• **CVE-2022-0185**: kernel - fs_context: heap overflow in legacy parameter handling |
| Affected Products | Red Hat Enterprise Linux for x86_64 - Extended Update Support 8.4 x86_64<br>Red Hat Enterprise Linux Server - AUS 8.4 x86_64<br>Red Hat Enterprise Linux for Power, little endian - Extended Update Support 8.4 ppc64le<br>Red Hat Enterprise Linux Server - TUS 8.4 x86_64<br>Red Hat Enterprise Linux Server (for IBM Power LE) - Update Services for SAP Solutions 8.4 ppc64le<br>Red Hat Enterprise Linux Server - Update Services for SAP Solutions 8.4 x86_64 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://access.redhat.com/errata/RHSA-2022:0231<br>https://access.redhat.com/security/cve/CVE-2021-4154<br>https://access.redhat.com/security/cve/CVE-2021-4155<br>https://access.redhat.com/security/cve/CVE-2022-0185 |

### 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.**