Advisory Alert

Alert Number: AAA20220404 **Date:** April 4, 2022

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Samba	**High**	Multiple Vulnerabilities

Description

Affected Product	**Samba**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-44141, CVE-2021-44142, CVE-2022-0336)
Description	Samba has released security updates to address vulnerabilities in multiple versions of Samba. • **CVE-2021-44141:** A malicious user could create a symlink to determine if a file or directory exists in an area of the server file system not exported under the share definition. Successful exploitation of this vulnerability could lead to disclosure of sensitive information. • **CVE-2021-44142:** Out-of-bounds vulnerability that allows attackers to remotely execute code on machines running a Samba server with a vulnerable configuration as root user. • **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. All versions of Samba prior to 4.13.17 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 https://www.samba.org/samba/security/CVE-2021-44141.html https://www.samba.org/samba/security/CVE-2021-44142.html https://www.samba.org/samba/security/CVE-2022-0336.html

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.