Advisory Alert

Alert Number: AAA20230403 **Date:** April 3, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Samba	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**Samba**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-0225, CVE-2023-0922, CVE-2023-0614)
Description	Samba has released a security updates addressing multiple vulnerabilities that exist in their versions. **CVE-2023-0225** - An incomplete access check on dnsHostName attribute allows authenticated, unprivileged users to delete this attribute from any object in the directory **CVE-2023-0922** - The Samba AD DC administration tool, when operating against a remote LDAP server, will by default send new or reset passwords in cleartext over a signed-only connection **CVE-2023-0614** - The vulnerability allows a remote user to gain access to sensitive information bypassing the implemented LDAP filters security restrictions in Samba AD DC. Samba recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	All versions of Samba since 4.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.samba.org/samba/security/CVE-2023-0225.html https://www.samba.org/samba/security/CVE-2023-0922.html https://www.samba.org/samba/security/CVE-2023-0614.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.