Advisory Alert

Alert Number: AAA20220511 **Date:** May 11, 2022

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Microsoft	**High**	Multiple Vulnerabilities
Zimbra	**High**	Inject Arbitrary Memcache Command

Description

Affected Product	Microsoft	
Severity	**High**	
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-21972, CVE-2022-21978, CVE-2022-22011, CVE-2022-22012, CVE-2022-22015, CVE-2022-22016, CVE-2022-22017, CVE-2022-22019, CVE-2022-22713, CVE-2022-23270, CVE-2022-23279, CVE-2022-24466, CVE-2022-26913, CVE-2022-26923, CVE-2022-26925, CVE-2022-26926, CVE-2022-26927, CVE-2022-26930, CVE-2022-26931, CVE-2022-26932, CVE-2022-26933, CVE-2022-26934, CVE-2022-26935, CVE-2022-26936, CVE-2022-26937, CVE-2022-26938, CVE-2022-26939, CVE-2022-26940, CVE-2022-29102, CVE-2022-29106, CVE-2022-29107, CVE-2022-29108, CVE-2022-29109, CVE-2022-29110, CVE-2022-29112, CVE-2022-29113, CVE-2022-29114, CVE-2022-29115, CVE-2022-29116, CVE-2022-29120, CVE-2022-29121, CVE-2022-29122, CVE-2022-29123, CVE-2022-29125, CVE-2022-29126, CVE-2022-29127, CVE-2022-29128, CVE-2022-29129, CVE-2022-29130, CVE-2022-29131, CVE-2022-29133, CVE-2022-29134, CVE-2022-29135, CVE-2022-29138, CVE-2022-29139, CVE-2022-29140, CVE-2022-29142, CVE-2022-29148, CVE-2022-29150, CVE-2022-29151, CVE-2022-29972, CVE-2022-30129)	
Description	Microsoft has issued Security Updates addressing multiple vulnerabilities that exists in variety of Microsoft products, features, and roles. Updates include defense-in-depth updates to help strengthen security-related aspects, in addition to security improvements for the vulnerabilities. Microsoft strongly advises to apply security fixes at earliest to avoid problems.	
Affected Products	.NET and Visual Studio Microsoft Exchange Server Microsoft Graphics Component Microsoft Local Security Authority Server (lsasrv) Microsoft Office Microsoft Office Excel Microsoft Office SharePoint Microsoft Windows ALPC Remote Desktop Client Role: Windows Fax Service Role: Windows Hyper-V Self-hosted Integration Runtime Tablet Windows User Interface Visual Studio Visual Studio Code Windows Active Directory Windows Address Book Windows Authentication Methods	Windows Cluster Shared Volume (CSV) Windows Failover Cluster Automation Server Windows Kerberos Windows Kernel Windows LDAP - Lightweight Directory Access Protocol Windows Media Windows Network File System Windows NTFS Windows Point-to-Point Tunneling Protocol Windows Print Spooler Components Windows Push Notifications Windows Remote Access Connection Manager Windows Remote Desktop Windows Remote Procedure Call Runtime Windows Server Service Windows Storage Spaces Controller Windows WLAN Auto Config Service Windows BitLocker
Officially Acknowledged by the Vendor	Yes	
Patch/ Workaround Released	Yes	
Reference	https://msrc.microsoft.com/update-guide/releaseNote/2022-May	

Affected Product	Zimbra
Severity	**High**
Affected Vulnerability	Inject Arbitrary Memcache Command (CVE-2022-27924)
Description	Zimbra has released security patch updates to address a vulnerability that exist in their products. **CVE-2022-27924** – This vulnerability allows an unauthenticated attacker to inject arbitrary memcache commands into a targeted instance. These memcache commands becomes unescaped, causing an overwrite of arbitrary cached entries.
Affected Products	Zimbra Collaboration Kepler 9.0.0 Zimbra Collaboration Joule 8.8.15
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://wiki.zimbra.com/wiki/Zimbra_Releases/9.0.0/P24.1#Security_Fixes https://wiki.zimbra.com/wiki/Zimbra_Releases/8.8.15/P31.1#Security_Fixes

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.