Advisory Alert

Alert Number: AAA20221012 **Date:** October 12, 2022

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Zimbra	**Critical**	Arbitrary file overwrite Vulnerability
Microsoft	**High**	Multiple Vulnerabilities
Zimbra	**Medium**	Multiple vulnerabilities
Citrix	**Medium**	Multiple Vulnerabilities
OpenSSL	**Low**	NULL encryption Vulnerability

Description

Affected Product	**Zimbra**
Severity	**Critical**
Affected Vulnerability	Arbitrary file overwrite Vulnerability (CVE-2022-41352)
Description	Zimbra has released security patch updates addressing an arbitrary file overwrite vulnerability that exist in their products.Using this vulnerability an attacker can upload arbitrary files through amavisd via a cpio loophole (extraction to /opt/zimbra/jetty/webapps/zimbra/public) that can leads to incorrect access to any other user accounts. This vulnerability have been fixed in this Zimbra Collaboration Suite patch update.
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/P27#Security_Fixes https://wiki.zimbra.com/wiki/Zimbra_Releases/8.8.15/P34#Security_Fixes

Affected Product	**Microsoft**	
Severity	**High**	
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-22035, CVE-2022-24504, CVE-2022-30198, CVE-2022-3304, CVE-2022-3307, CVE-2022-3308, CVE-2022-3310, CVE-2022-3311, CVE-2022-3313, CVE-2022-3315, CVE-2022-3316, CVE-2022-3317, CVE-2022-33634, CVE-2022-33635, CVE-2022-3370, CVE-2022-3373, CVE-2022-34689, CVE-2022-35770, CVE-2022-35829, CVE-2022-37965, CVE-2022-37968, CVE-2022-37970, CVE-2022-37971, CVE-2022-37973, CVE-2022-37974, CVE-2022-37975, CVE-2022-37976, CVE-2022-37978, CVE-2022-37979, CVE-2022-37980, CVE-2022-37981, CVE-2022-37982, CVE-2022-37983, CVE-2022-37984, CVE-2022-37985, CVE-2022-37986, CVE-2022-37987, CVE-2022-37988, CVE-2022-37989, CVE-2022-37990, CVE-2022-37991, CVE-2022-37993, CVE-2022-37994, CVE-2022-37995, CVE-2022-37996, CVE-2022-37997, CVE-2022-37999, CVE-2022-38000, CVE-2022-38001, CVE-2022-38016, CVE-2022-38017, CVE-2022-38021, CVE-2022-38022, CVE-2022-38025, CVE-2022-38026, CVE-2022-38027, CVE-2022-38028, CVE-2022-38029, CVE-2022-38030, CVE-2022-38031, CVE-2022-38032, CVE-2022-38033, CVE-2022-38034, CVE-2022-38037, CVE-2022-38038, CVE-2022-38039, CVE-2022-38040, CVE-2022-38042, CVE-2022-38043, CVE-2022-38044, CVE-2022-38045, CVE-2022-38046, CVE-2022-38047, CVE-2022-38048, CVE-2022-38049, CVE-2022-38050, CVE-2022-38051, CVE-2022-38053, CVE-2022-41031, CVE-2022-41032, CVE-2022-41033, CVE-2022-41034, CVE-2022-41035, CVE-2022-41036, CVE-2022-41037, CVE-2022-41038, CVE-2022-41042, CVE-2022-41043, CVE-2022-41081, CVE-2022-41083)	
Description	Microsoft has released Security Updates addressing multiple vulnerabilities that exists with multiple Microsoft products, features and roles. In addition to security changes for the vulnerabilities, updates include defense in depth updates to help improve security related features. It is highly recommended by Microsoft to apply necessary security fixes at earliest to avoid issues	
Affected Products	Active Directory Domain Services Azure Azure Arc Client Server Run-time Subsystem (CSRSS) Microsoft Edge (Chromium-based) Microsoft Graphics Component Microsoft Office Microsoft Office SharePoint Microsoft Office Word Microsoft WDAC OLE DB provider for SQL NuGet Client Remote Access Service Point-to-Point Tunneling Protocol Role: Windows Hyper-V Service Fabric Visual Studio Code Windows Active Directory Certificate Services Windows ALPC Windows CD-ROM Driver Windows COM+ Event System Service Windows Connected User Experiences and Telemetry Windows CryptoAPI Windows Defender Windows DHCP Client Windows Distributed File System (DFS) Windows DWM Core Library Windows Event Logging Service Windows Group Policy	Windows Group Policy Preference Client Windows Internet Key Exchange (IKE) Protocol Windows Kernel Windows Local Security Authority (LSA) Windows Local Security Authority Subsystem Service (LSASS) Windows Local Session Manager (LSM) Windows NTFS Windows NTLM Windows ODBC Driver Windows Perception Simulation Service Windows Point-to-Point Tunneling Protocol Windows Portable Device Enumerator Service Windows Print Spooler Components Windows Resilient File System (ReFS) Windows Secure Channel Windows Security Support Provider Interface Windows Server Remotely Accessible Registry Keys Windows Server Service Windows Storage Windows TCP/IP Windows USB Serial Driver Windows Web Account Manager Windows Win32K Windows WLAN Service Windows Workstation Service
Officially Acknowledged by the Vendor	Yes	
Patch/ Workaround Released	Yes	
Reference	https://msrc.microsoft.com/update-guide/releaseNote/2022-Oct	

Affected Product	**Zimbra**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-41348, CVE-2022-41350, CVE-2022-41349, CVE-2022-41351)
Description	Zimbra has released security patch updates addressing multiple vulnerabilities that exist in their products. Exploitation of the most severe vulnerabilities could cause information disclosure. These vulnerabilities have been fixed in this Zimbra Collaboration Suite patch update.
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/P27#Security_Fixes https://wiki.zimbra.com/wiki/Zimbra_Releases/8.8.15/P34#Security_Fixes

Affected Product	**Citrix**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-33748, CVE-2022-33749)
Description	Citrix has released Security Updates addressing multiple Vulnerabilities that exist in their products. **CVE-2022-33748** - A malicious privileged user in a guest VM working in collaboration with a malicious privileged user in another guest VM can cause the host to crash or become unresponsive. **CVE-2022-33749** - A malicious unauthenticated user on the management network may be able to cause the management service on the host to crash or become unresponsive. Citrix recommends to apply necessary security fixes at earliest to avoid issues
Affected Products	Citrix Hypervisor 8.2 LTSR CU1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.citrix.com/article/CTX465146/citrix-hypervisor-security-bulletin-for-cve202233748-cve202233749

Affected Product	**OpenSSL**
Severity	**Low**
Affected Vulnerability	NULL encryption Vulnerability (CVE-2022-3358)
Description	OpenSSL has released Security Updates addressing a NULL encryption vulnerability that exist in their products. The vulnerability exists due to an error in openssl implementation when handling legacy custom ciphers with NID_undef passed to the EVP_EncryptInit_ex2(), EVP_DecryptInit_ex2() and EVP_CipherInit_ex2() functions. Under certain conditions openssl can fail to select a proper cipher and use NULL instead, which corresponds to sending data in plain text. OpenSSL recommends to apply necessary security fixes at earliest to avoid issues
Affected Products	OpenSSL: 3.0.0 - 3.0.5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.openssl.org/news/secadv/20221011.txt

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.