How

Advisory Alert

Alert Number: AAA20220810 **Date:** August 10, 2022

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Microsoft	**Critical**	Multiple Vulnerabilities
Microsoft	**High**	Multiple Vulnerabilities
VMware	**High**, **Medium**	Multiple Vulnerabilities
SonicWALL	**High**	Multiple Vulnerabilities
Citrix	**Low**	Security Update

Description

Affected Product	**Microsoft**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-34691, CVE-2022-33646, CVE-2022-21980, CVE-2022-24516, CVE-2022-24477, CVE-2022-35752, CVE-2022-35753, CVE-2022-34696, CVE-2022-35804, CVE-2022-30133, CVE-2022-35744, CVE-2022-35745, CVE-2022-35766, CVE-2022-35794, CVE-2022-34714, CVE-2022-34702, CVE-2022-35767)
Description	Microsoft has released Security Updates addressing multiple critical 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 Batch Node Agent Microsoft Exchange Server Remote Access Service Point-to-Point Tunneling Protocol Role: Windows Hyper-V Windows Kernel Windows Point-to-Point Tunneling Protocol Windows Secure Socket Tunneling Protocol (SSTP)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://msrc.microsoft.com/update-guide/releaseNote/2022-Aug

Affected Product	**Microsoft**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-34716, CVE-2022-34685, CVE-2022-34686, CVE-2022-35773, CVE-2022-35779, CVE-2022-35806, CVE-2022-34687, CVE-2022-30176, CVE-2022-30175, CVE-2022-35791, CVE-2022-35818, CVE-2022-35809, CVE-2022-35789, CVE-2022-35815, CVE-2022-35817, CVE-2022-35816, CVE-2022-35814, CVE-2022-35785, CVE-2022-35812, CVE-2022-35811, CVE-2022-35784, CVE-2022-35810, CVE-2022-35813, CVE-2022-35788, CVE-2022-35783, CVE-2022-35786, CVE-2022-35787, CVE-2022-35819, CVE-2022-35781, CVE-2022-35775,CVE-2022-35790, CVE-2022-35780, CVE-2022-35799, CVE-2022-35772, CVE-2022-35800, CVE-2022-35774, CVE-2022-35802, CVE-2022-35782, CVE-2022-35824, CVE-2022-35801, CVE-2022-35808, CVE-2022-35776, CVE-2022-35807, CVE-2022-35821, CVE-2022-35760, CVE-2022-35820, CVE-2022-35796, CVE-2022-33649 CVE-2022-2618, CVE-2022-2616, CVE-2022-2617, CVE-2022-2619, CVE-2022-2622, CVE-2022-2623, CVE-2022-33636, CVE-2022-2621, CVE-2022-2615, CVE-2022-2604, CVE-2022-2605, CVE-2022-2624 CVE-2022-2603, CVE-2022-2606, CVE-2022-2612, CVE-2022-2614, CVE-2022-2610, CVE-2022-2611, CVE-2022-34692, CVE-2022-21979, CVE-2022-30134, CVE-2022-34717, CVE-2022-33648, CVE-2022-33631, CVE-2022-35742, CVE-2022-34713, CVE-2022-35743, CVE-2022-35769, CVE-2022-34690, CVE-2022-35751, CVE-2022-33640, CVE-2022-35827, CVE-2022-35777, CVE-2022-35825, CVE-2022-35826, CVE-2022-30144, CVE-2022-35750, CVE-2022-35757, CVE-2022-35771, CVE-2022-34705, CVE-2022-34710, CVE-2022-34709, CVE-2022-34704, CVE-2022-34712, CVE-2022-35746 CVE-2022-35749, CVE-2022-35795, CVE-2022-35797, CVE-2022-35748, CVE-2022-35756, CVE-2022-35761, CVE-2022-35768, CVE-2022-34708, CVE-2022-34707, CVE-2022-30197, CVE-2022-35758, CVE-2022-34706, CVE-2022-35759, CVE-2022-34715, CVE-2022-33670, CVE-2022-34703, CVE-2022-35747, CVE-2022-35793,CVE-2022-35755, CVE-2022-34301, CVE-2022-34302, CVE-2022-34303, CVE-2022-34701, CVE-2022-35762, CVE-2022-35765, CVE-2022-35792, CVE-2022-35763, CVE-2022-35764, CVE-2022-35754, CVE-2022-30194, CVE-2022-34699)
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	.NET Core Azure Real Time Operating System Azure Site Recovery Azure Sphere Microsoft ATA Port Driver Microsoft Bluetooth Driver Microsoft Edge (Chromium-based) Microsoft Exchange Server Microsoft Office Microsoft Office Excel Microsoft Office Outlook Microsoft Windows Support Diagnostic Tool (MSDT) Remote Access Service Point-to-Point Tunneling Protocol Role: Windows Fax Service Role: Windows Hyper-V System Center Operations Manager Visual Studio Windows Bluetooth Service Windows Canonical Display Driver Windows Cloud Files Mini Filter Driver Windows Defender Credential Guard Windows Digital Media Windows Error Reporting Windows Hello Windows Internet Information Services Windows Kerberos Windows Kernel Windows Local Security Authority (LSA) Windows Network File System Windows Partition Management Driver Windows Point-to-Point Tunneling Protocol Windows Print Spooler Components Windows Secure Boot Windows Secure Socket Tunneling Protocol (SSTP) Windows Storage Spaces Direct Windows Unified Write Filter Windows WebBrowser Control Windows Win32K
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://msrc.microsoft.com/update-guide/releaseNote/2022-Aug

Affected Product	**VMware**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities(CVE-2022-31672, CVE-2022-31673, CVE-2022-31674, CVE-2022-31675, CVE-2022-22983)
Description	VMware has released Security Updates addressing multiple vulnerabilities in their products, including the Privilege Escalation Vulnerability, Information Disclosure Vulnerability, Authentication Bypass Vulnerability, and Unprotected Storage of Credentials vulnerability. VMware highly recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	VMware vRealize Operations 8.x VMware Workstation 16.x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.vmware.com/security/advisories/VMSA-2022-0022.html https://www.vmware.com/security/advisories/VMSA-2022-0023.html

Affected Product	**SonicWALL**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-33909, CVE-2022-0847)
Description	SonicWALL has released a security update addressing multiple vulnerabilities that exist in SMA1000 platform. **CVE-2021-33909 -** Due to fs/seq_file.c in the Linux kernel 3.16 through 5.13.x before 5.13.4 does not properly restrict seq buffer allocations. An out-of-bounds write flaw was exists in the Linux kernel's seq_file in the Filesystem layer. This flaw allows a local attacker with a user privilege to gain access to out-of-bound memory, leading to a system crash, leak of internal kernel information and can escalate privileges. **CVE-2022-0847-** A flaw was found in the way the "flags" member of the new pipe buffer structure was lacking proper initialization in copy_page_to_iter_pipe and push_pipe functions in the Linux kernel and could thus contain stale values. An unprivileged local user could use this flaw to write to pages in the page cache backed by read only files and as such escalate their privileges on the system SonicWall highly recommended to apply necessary fixes at earliest to avoid issues.
Affected Products	SonicWall SMA1000 12.4.2-02044 and earlier versions
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2022-0015

Affected Product	**Citrix**
Severity	**Low**
Affected Vulnerability	Security Update (CVE-2022-33745)
Description	Citrix has released security update to address a flaw found in Citrix Hypervisor 7.1 LTSR CU2 products. The flow may allow a privileged code in a PV guest VM to fail to perform management operations. Citrix highly recommended to apply necessary fixes at earliest to avoid issues.
Affected Products	Citrix Hypervisor 7.1 LTSR CU2 Citrix XenServer
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.citrix.com/article/CTX463455/citrix-hypervisor-security-bulletin-for-cve202233745

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.