Advisory Alert

Alert Number: AAA20210714 **Date:** July 14, 2021

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Microsoft	**Critical**	Multiple Vulnerabilities
Solarwinds	**Critical**	Remote memory escape vulnerability
Intel	**High**	Privilege escalation vulnerability
Citrix	**High**	Privilege escalation vulnerability
VMWare	**High**	Multiple Vulnerabilities

Description

Affected Product	Microsoft	
Severity	**Critical**	
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-31206,CVE-2021-31947,CVE-2021-31961,CVE-2021-33749,CVE-2021-33750,CVE-2021-33752,CVE-2021-33753,CVE-2021-33756,CVE-2021-33757,CVE-2021-33760,CVE-2021-33763,CVE-2021-33764,CVE-2021-33767,CVE-2021-33768,CVE-2021-33775,CVE-2021-33776,CVE-2021-33777,CVE-2021-33778,CVE-2021-33783,CVE-2021-34440,CVE-2021-34447,CVE-2021-34451,CVE-2021-34452,CVE-2021-34454,CVE-2021-34457,CVE-2021-34458,CVE-2021-34464,CVE-2021-34469,CVE-2021-34470,CVE-2021-34474,CVE-2021-34491,CVE-2021-34496,CVE-2021-34497,CVE-2021-34500,CVE-2021-34501,CVE-2021-34507,CVE-2021-34509,CVE-2021-34518,CVE-2021-34519,CVE-2021-34521,CVE-2021-34522,CVE-2021-34527)	
Description	Microsoft has released security updates addressing multiple vulnerabilities that exists in their products. The most severe could cause privilege escalation, remote code execution, security by pass and information disclosure. Microsoft highly recommends to apply necessary security fixes to avoid issues.	
Affected Products	Common Internet File System Dynamics Business Central Control Microsoft Bing Microsoft Dynamics Microsoft Exchange Server Microsoft Graphics Component Microsoft Office Microsoft Office Excel Microsoft Office SharePoint Microsoft Scripting Engine Microsoft Windows Codecs Library Microsoft Windows DNS Microsoft Windows Media Foundation OpenEnclave Power BI Role: DNS Server Role: Hyper-V Visual Studio Code Visual Studio Code - .NET Runtime Visual Studio Code - Maven for Java Extension Windows Active Directory Windows Address Book Windows AF_UNIX Socket Provider Windows AppContainer Windows AppX Deployment Extensions Windows Authenticode	Windows Cloud Files Mini Filter Driver Windows Console Driver Windows Defender Windows Desktop Bridge Windows Event Tracing Windows File History Service Windows Hello Windows HTML Platform Windows Installer Windows Kernel Windows Key Distribution Center Windows Local Security Authority Subsystem Service Windows MSHTML Platform Windows Partition Management Driver Windows PFX Encryption Windows Print Spooler Components Windows Projected File System Windows Remote Access ConnectionManager Windows Remote Assistance Windows Secure Kernel Mode Windows Security Account Manager Windows Shell Windows SMB Windows Storage Spaces Controller Windows TCP/IP Windows Win32K
Officially Acknowledged by the Vendor	Yes	
Patch/ Workaround Released	Yes	
Reference	https://msrc.microsoft.com/update-guide/releaseNote/2021-Jul	

Affected Product	Solarwinds
Severity	**Critical**
Affected Vulnerability	Remote memory escape vulnerability (CVE-2021-35211)
Description	Solarwinds has released security updates addressing remote memory escape vulnerability that exists in their products. After successfully exploitation this vulnerability an attacker could run arbitrary code with privileges and then install programs, view/change/delete data or run programs on the affected system. It is highly recommended by solarwinds to apply necessary security fixes to avoid issues.
Affected Products	Serv-U 15.2.3 HF1 and all prior Serv-U versions
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.solarwinds.com/trust-center/security-advisories/cve-2021-35211

Affected Product	Intel
Severity	**High**
Affected Vulnerability	Privilege escalation vulnerability (CVE-2021-0144)
Description	Intel has released security updates addressing privilege escalation vulnerability that exists in their products. Insecure default variable initialization for the Intel BSSA DFT feature might allow a privileged user to potentially enable an privilege escalation locally. It is highly recommended by Intel to apply necessary security fixes to avoid issues.
Affected Products	2nd Generation Intel® Xeon® Scalable Processors Intel® Xeon® Scalable Processors Intel® Core™ X-series Processors Intel® Xeon® Processor W Family Intel® Xeon® Processor D Family Intel® Xeon® Processor E5 v4 Family Intel® Xeon® Processor E5 v3 Family
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00525.html

Affected Product	Citrix
Severity	**High**
Affected Vulnerability	Privilege escalation vulnerability (CVE-2021-22928)
Description	Citrix has released security updates addressing privilege escalation vulnerability that exists in their products. Successful exploitation of this vulnerability could allow a user of a Windows VDA that has either Citrix Profile Management or Citrix Profile Management WMI Plugin installed, to escalate their privilege level on that Windows VDA to SYSTEM. It is highly recommended by Citrix to apply necessary security fixes to avoid issues.
Affected Products	Citrix Virtual Apps and Desktops 2106 and earlier versions Citrix Virtual Apps and Desktops 1912 LTSR CU3 and earlier versions of 1912 LTSR Citrix XenApp / XenDesktop 7.15 LTSR CU7 and earlier versions of 7.15 LTSR
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.citrix.com/article/CTX319750

Affected Product	VMWare
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-21994,CVE-2021-21995,CVE-2021-22000)
Description	VMWare has released security updates addressing multiple vulnerabilities that exists in their products. CVE-2021-21994 – An attacker with network access to port 5989 on ESXi may exploit this issue to bypass SFCB authentication by sending a specially crafted request. CVE-2021-21995 - An attacker with network access to port 427 on ESXi may be able to trigger a heap out-of-bounds read in OpenSLP service resulting in a denial-of-service condition. CVE-2021-22000 - An attacker with non-administrative privileges may exploit this vulnerability to elevate privileges to administrator level on the Windows operating system having VMware ThinApp installed on it It is highly recommended by VMWare to apply necessary security fixes to avoid issues.
Affected Products	VMware ESXi VMware Cloud Foundation (Cloud Foundation) VMware ThinApp
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.vmware.com/security/advisories/VMSA-2021-0014.html https://www.vmware.com/security/advisories/VMSA-2021-0015.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.