Advisory Alert

Alert Number: AAA20220714 **Date:** July 14, 2022

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

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

Description

Affected Product	**Juniper**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities
Description	Juniper has released security patch updates addressing multiple vulnerabilities including critical and high vulnerabilities that exists in their multiple products. An attacker could use these vulnerabilities to gain access to systems and perform malicious activities. Most of the vulnerabilities are found in the Junos OS. It is highly recommended to apply necessary fixes at earliest to the Juniper products to avoid issues
Affected Products	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://supportportal.juniper.net/s/global-search/%40uri?language=en_US

Affected Product	**Microsoft**	
Severity	**High**	
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-21845, CVE-2022-22022, CVE-2022-22023, CVE-2022-22024, CVE-2022-22026, CVE-2022-22027, CVE-2022-22028, CVE-2022-22029, CVE-2022-22031, CVE-2022-22034, CVE-2022-22036, CVE-2022-22037, CVE-2022-22038, CVE-2022-22039, CVE-2022-22040, CVE-2022-22041, CVE-2022-22042, CVE-2022-22043, CVE-2022-22045, CVE-2022-22047, CVE-2022-22048, CVE-2022-22049, CVE-2022-22050, CVE-2022-22711, CVE-2022-2294, CVE-2022-2295, CVE-2022-23816, CVE-2022-23825, CVE-2022-27776, CVE-2022-30181, CVE-2022-30187, CVE-2022-30202, CVE-2022-30203, CVE-2022-30205, CVE-2022-30206, CVE-2022-30209, CVE-2022-30211, CVE-2022-30212, CVE-2022-30213, CVE-2022-30214, CVE-2022-30215, CVE-2022-30216, CVE-2022-30220, CVE-2022-30221, CVE-2022-30222, CVE-2022-30223, CVE-2022-30224, CVE-2022-30225, CVE-2022-30226, CVE-2022-33632, CVE-2022-33633, CVE-2022-33637, CVE-2022-33641, CVE-2022-33642, CVE-2022-33643, CVE-2022-33644, CVE-2022-33650, CVE-2022-33651, CVE-2022-33652, CVE-2022-33653, CVE-2022-33654, CVE-2022-33655, CVE-2022-33656, CVE-2022-33657, CVE-2022-33658, CVE-2022-33659, CVE-2022-33660, CVE-2022-33661, CVE-2022-33662, CVE-2022-33663, CVE-2022-33664, CVE-2022-33665, CVE-2022-33666, CVE-2022-33667, CVE-2022-33668, CVE-2022-33669, CVE-2022-33671, CVE-2022-33672, CVE-2022-33673, CVE-2022-33674, CVE-2022-33675, CVE-2022-33676, CVE-2022-33677, CVE-2022-33678)	
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	AMD CPU Branch Azure Site Recovery Azure Storage Library Microsoft Defender for Endpoint Microsoft Edge (Chromium-based) Microsoft Graphics Component Microsoft Office Open Source Software Role: DNS Server Role: Windows Fax Service Role: Windows Hyper-V Skype for Business and Microsoft Lync Windows Active Directory Windows Advanced Local Procedure Call Windows BitLocker Windows Boot Manager Windows Client/Server Runtime Subsystem	Windows Connected Devices Platform Service Windows Credential Guard Windows Fast FAT Driver Windows Fax and Scan Service Windows Group Policy Windows IIS Windows Kernel Windows Media Windows Network File System Windows Performance Counters Windows Point-to-Point Tunneling Protocol Windows Portable Device Enumerator Service Windows Print Spooler Components Windows Remote Procedure Call Runtime Windows Security Account Manager Windows Server Service Windows Shell Windows Storage
Officially Acknowledged by the Vendor	Yes	
Patch/ Workaround Released	Yes	
Reference	https://msrc.microsoft.com/update-guide/releaseNote/2022-Jul	

Affected Product	**Citrix**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-23825, CVE-2022-29900)
Description	Citrix has released security updates to address multiple flaws that exists on the AMD CPUs that could allow code inside a guest VM to guess the contents of RAM memory elsewhere on the host. This flaws only affects if the Citrix hypervisor is running on the affected AMD CPUs. Citrix highly recommended to apply necessary fixes at earliest to the Citrix products to avoid issues.
Affected Products	Citrix Hypervisor 8.2 Citrix XenServer 7.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.citrix.com/article/CTX461397/citrix-hypervisor-security-bulletin-for-cve202223816-and-cve202223825

Affected Product	**Cpanel**
Severity	**Medium**
Affected Vulnerability	Security Update (CVE-2022-31627)
Description	Cpanel has released its Security Updates which address of EasyApache 4 with PHP product. These updates provide targeted changes to address security concerns.
Affected Products	All versions of PHP 8.1 through 8.1.7.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://news.cpanel.com/easyapache-july-13-release/

Affected Product	**VMware**
Severity	**Medium, Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-29901, CVE-2022-28693, CVE-2022-23816, CVE-2022-23825, CVE-2022-31654, CVE-2022-31655, CVE-2022-22982)
Description	VMware has released Security Updates addressing multiple vulnerabilities including Return Stack Buffer Underflow, Branch Type Confusion, Cross Site Scripting, and server-side request forgery (SSRF) that contains in their products which leads attackers to perform malicious activities. VMware highly recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	VMware ESXi VMware Cloud Foundation VMware vRealize Log Insight VMware vCenter Server (vCenter Server) VMware Cloud Foundation (Cloud Foundation)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.vmware.com/security/advisories/VMSA-2022-0020.html https://www.vmware.com/security/advisories/VMSA-2022-0019.html https://www.vmware.com/security/advisories/VMSA-2022-0018.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.