Advisory Alert

Alert Number: AAA20210528 **Date:** May 28, 2021

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
VMware	**Critical**	Remote Code Execution
Juniper	**Critical, High**	Multiple Vulnerabilities
Drupal	**Critical**	Cross Site Scripting
IBM	**High**	Multiple Vulnerabilities
SonicWall	**High**	Command Injection
Microsoft	**High**	Multiple Vulnerabilities
Nginx	**Medium**	Arbitrary Code Execution
Joomla	**Low**	Multiple Vulnerabilities

Description

Affected Product	VMware
Severity	**Critical**
Affected Vulnerability	Remote code execution (CVE-2021-21985, CVE-2021-21986)
Description	The vSphere Client (HTML5) Virtual SAN Health Testing Plugin contains remote code execution victim due to invalidation of input which is basically enabled in the vCenter server.A malicious actor with network access to port 443 may exploit this issue to execute commands with unrestricted privileges on the underlying operating system that hosts vCenter Server
Affected Products	VMware vCenter Server (vCenter Server)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.vmware.com/security/advisories/VMSA-2021-0010.html

Affected Product	Juniper
Severity	**Critical , High**
Affected Vulnerability	Multiple vulnerabilities (CVE-2021-0268, CVE-2021-0254)
Description	CVE-2021-0268 - An Improper Neutralization of CRLF Sequences in HTTP Headers weakness in J-web of Juniper. Junos OS leads to buffer overflows, segment faults, or other impacts allowing the attacker to modify the integrity of the device and exfiltration information from the device without authentication. CVE-2021-0254 - A buffer size validation vulnerability in the overlayd service of Juniper Networks Junos OS may allow an unauthenticated remote attacker to send specially crafted packets to the device, triggering a partial Denial of Service (DoS) condition, or leading to remote code execution (RCE).
Affected Products	Junos OS 15.1, 17.3, 17.4, 18.1, 18.2, 18.3, 18.4, 19.1, 19.2, 19.3, 19.4, 20.1, 20.2, 20.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11159&cat=SIRT_1&actp=LIST https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11147&cat=SIRT_1&actp=LIST

Affected Product	Drupal
Severity	**Critical**
Affected Vulnerability	Cross Site Scripting
Description	Drupal core uses the third-party CKEditor library. There is a bug in the HTML configuration that could cause an XSS attack on this library. CKEditor 4.16.1 and later versions include the fixes.Users of the CKEditor library need to update their third-party code through methods other than DKpal core. Drupal has recommended upgrading there vulnerable versions
Affected Products	Drupal 9.1 Drupal 9.0 Drupal 8.9
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.drupal.org/sa-core-2021-003

Affected Product	IBM
Severity	**High**
Affected Vulnerability	Multiple vulnerabilities
Description	IBM Db2 for Linux, UNIX and Windows Db2 Connect Server could allow a local user to execute arbitrary code and conduct DLL hijacking attacks.
Affected Products	IBM Db2 V9.7, V10.1, V10.5, V11.1, and V11.5 editions on Windows are affected.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/6456029

Affected Product	SonicWall
Severity	**High**
Affected Vulnerability	Command Injection (CVE-2021-20026)
Description	The insecurity of the Sonicwall NSM On-Prime product allows an authenticated attacker to inject OS commands using an HTTP request.
Affected Products	NSM On-Prem 2.2.0-R10 and earlier versions
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0014

Affected Product	Microsoft
Severity	**High**
Affected Vulnerability	Multiple vulnerabilities
Description	Microsoft has released its May 2021 Security Updates which address multiple Vulnerabilities across several of products, which an attacker could use to gain control of an affected system. Microsoft highly recommends to apply relevant patches at earliest to avoid issues.
Affected Products	.NET Core & Visual Studio HTTP.sys Internet Explorer Microsoft Exchange Server Microsoft Graphics Component Microsoft Office Microsoft Office Access Microsoft Office Excel Microsoft Office SharePoint Microsoft Office Word Microsoft Windows Codecs Library Microsoft Windows IrDA Hyper-V Visual Studio Visual Studio Code Windows Container Isolation FS Filter Driver Windows Container Manager Service Windows Cryptographic Services Windows RDP Client Windows SMB Windows SSDP Service Windows Wireless Networking
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://msrc.microsoft.com/update-guide/releaseNote/2021-May

Affected Product	Nginx
Severity	**Medium**
Affected Vulnerability	Arbitrary Code Execution (CVE-2021-23017)
Description	Nginx has identified a security issue with the resolver, which allows the attacker to overwrite 1-byte memory using a specially designed DNS response, resulting in worker process crash or, potentially, arbitrary code execution.The issue only affects Nginx if the "resolver" directive is used in the configuration file. Also, this attack is only possible if UDP packets can be built from the attack DNS server.
Affected Products	Nginx 0.6.18 - 1.20.0.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	http://nginx.org/en/security_advisories.html http://mailman.nginx.org/pipermail/nginx-announce/2021/000300.html?_ga=2.185648800.88681853.1622171770-203159532.1607228800

Affected Product	Joomla
Severity	**Low**
Affected Vulnerability	Multiple vulnerabilities (CVE-2021-26032, CVE-2021-26033, CVE-2021-26034)
Description	CVE-2021-26032 - Media Helper Uploadable Activable Block List HTML is missing and leads to XSS Attack Vectors CVE-2021-26033, CVE-2021-26034 - A missing token check causes a CSRF vulnerability in the AJAX reordering endpoint or in data download endpoints in com_banners and com_sysinfo.
Affected Products	Joomla CMS versions 3.0.0 - 3.9.26
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://developer.joomla.org/security-centre/

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.