TLP: White[1]

Security Bulletin – August 2020

Dear Constituents,

Please find below our monthly roundup of security vulnerabilities for your information and necessary actions to secure your network and assets.

Vulnerabilities with Active Exploits in the Wild

Cisco Data Center Network Manager Authentication Bypass Vulnerability *(CVE-2020-3382)*

Severity: **HIGH**

Description

A vulnerability in the REST API of Cisco Data Center Network Manager (DCNM)

How it works

It will allow an unauthenticated, remote attacker to bypass authentication and execute arbitrary actions with administrative privileges on an affected device.

The vulnerability exists because different installations share a static encryption key. An attacker could exploit this vulnerability by using the static key to craft a valid session token. A successful exploit could allow the attacker to perform arbitrary actions through the REST API with administrative privileges.

What to do

Cisco has release the software updates that address the vulnerability.

Reference

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dcnm-bypass-dyEejUMs

IBM WebSphere Application Server Remote Code Execution Vulnerability *(CVE-2020-4534)*

Severity: **HIGH**

Description

IBM WebSphere Application Server could allow a local authenticated attacker to gain elevated privileges on the system.

How it works

This is caused by improper handling of UNC paths. By scheduling a task with a specially-crafted UNC path, an attacker could exploit this vulnerability to execute arbitrary code with higher privileges.

What to do

1 CERT Tonga adopts the Traffic Light Protocol

Always be sure to apply appropriate security updates recommended by IBM

Reference

https://exchange.xforce.ibmcloud.com/vulnerabilities/182808

https://www.ibm.com/support/pages/node/6255074

Cisco IP Cameras Cisco Discovery Protocol Remote Code Execution Vulnerabilities *(CVE-2020-3506)* Severity: **HIGH**

Description

Multiple vulnerabilities in the Cisco Discovery Protocol implementation for Cisco Video Surveillance 8000 Series IP Cameras.

How it works

It could allow an unauthenticated attacker to execute code remotely or cause a reload of an affected IP camera. These vulnerabilities are due to missing checks when the IP cameras process a Cisco Discovery Protocol packet. An attacker could exploit these vulnerabilities by sending a malicious Cisco Discovery Protocol packet to the targeted IP camera.

What to do

Cisco has released software updates that address these vulnerabilities.

Reference

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipcameras-rce-dos-uPyJYxN3

Adobe Acrobat Reader User After Free Vulnerability *(CVE-2020-9715)* Severity: **HIGH**

Description

A use-after-free vulnerability could allow remote attackers to execute arbitrary code on affected installations of Adobe Acrobat Reader DC.

How it works

The specific flaw exists within the handling of ES Object data objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process.

What to do

Adobe recommends users update their software installations to the latest versions

Reference

https://helpx.adobe.com/security/products/acrobat/apsb20-48.html

Trend Micro Rootkit Driver Input Validation Vulnerability *(CVE-2020-8607)* Severity: **HIGH**

Description

An input validation vulnerability found in multiple Trend Micro products

How it works

It utilizes a particular version of a specific rootkit protection driver could allow an attacker in user-mode with administrator permissions to abuse the driver to modify a kernel address that may cause a system crash or potentially lead to code execution in kernel mode.

An attacker must already have obtained administrator access on the target machine (either legitimately or via a separate unrelated attack) to exploit this vulnerability.

What to do

Trend Micro has released solutions to address the issue.

Reference

https://success.trendmicro.com/solution/000260713

Cisco AnyConnect Secure Mobility Client for Windows DLL Hijacking Vulnerability*(CVE-2020-3433)* Severity: **HIGH**

Description

A vulnerability in the interprocess communication (IPC) channel of Cisco AnyConnect Secure Mobility Client for Windows.

How it works

The vulnerability is due to insufficient validation of resources that are loaded by the application at run time. An attacker could exploit this vulnerability by sending a crafted IPC message to the AnyConnect process. A successful exploit could allow the attacker to execute arbitrary code on the affected machine with *SYSTEM* privileges. To exploit this vulnerability, the attacker would need to have valid credentials on the Windows system.

What to do

Cisco has released software updates that address these vulnerabilities.

Reference

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-anyconnect-dll-F26WwJW

Cisco NX-OS Software Border Gateway Protocol Multicast VPN Session Denial of Service Vulnerability*(CVE-2020-3398)* Severity: **HIGH**

Description

A vulnerability in the Border Gateway Protocol (BGP) Multicast VPN (MVPN) implementation of Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause a BGP

session to repeatedly reset, causing a partial denial of service condition due to the BGP session being down.

How it works

The vulnerability is due to incorrect parsing of a specific type of BGP MVPN update message. An attacker could exploit this vulnerability by sending this BGP MVPN update message to a targeted device. A successful exploit could allow the attacker to cause the BGP peer connections to reset, which could lead to BGP route instability and impact traffic. The incoming BGP MVPN update message is valid but is parsed incorrectly by the NX-OS device, which could send a corrupted BGP update to the configured BGP peer.

What to do

Cisco has released software updates that address this vulnerability

Reference

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxosbgp-mvpn-dos-K8kbCrJp

Microsoft Scripting Engine Memory Corruption Vulnerability *(CVE-2020-1380)* Severity: HIGH

Description

A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user.

How it works

An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

What to do

Apply appropriate security updates as recommended by Microsoft

Reference

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1380

Microsoft Windows Media Remote Code Execution Vulnerability *(CVE-2020-1339)* Severity: HIGH

Description

A remote code execution vulnerability exists when Windows Media Audio Codec improperly handles objects. An attacker who successfully exploited the vulnerability could take control of an affected system.

How it works

There are multiple ways an attacker could exploit the vulnerability, such as by convincing a user to open a specially crafted document, or by convincing a user to visit a malicious webpage.

What to do

Apply appropriate security updates as recommended by Microsoft

Reference

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1339

Qualcomm Out-Of-Bounds Memory Corruption Vulnerability *(CVE-2020-3698)* Severity: HIGH

Description

A vulnerability that could be exploited in Qualcomm

How it works

An Out of bound write happens in the component QoS DSCP when mapping due to improper input validation for data received from association response frame in Qualcomm Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music and Snapdragon Wearables (Chip Software).

What to do

Apply appropriate security updates recommended by Qualcomm

Reference

https://www.qualcomm.com/company/product-security/bulletins/july-2020-security-bulletin

vBulletin Remote Code Execution Vulnerability *(CVE-2019-16759)* Severity: HIGH

Description

A vulnerability found and could be exploited in vBulletin

How it works

vBulletin allows remote command execution via the widgetConfig[code] parameter in an ajax/render/widget_php routestring request. The vulnerability was disclosed through an 18-line exploit that was published on Monday by an unidentified person. The exploit allows unauthenticated attackers to remotely execute malicious code on just about any vBulletin server.

What to do

Apply appropriate security updates recommended by vBulletin

Reference

http://seclists.org/fulldisclosure/2020/Aug/5

Other Vulnerabilities with known Exploits

GRUB2 bootloader Buffer Overflow Vulnerability (CVE-2020-10713) Severity: **MEDIUM**

Description: A flaw was found in grub2, prior to version 2.06. An attacker may use the GRUB 2 flaw to hijack and tamper the GRUB verification process. This flaw also allows the bypass of Secure Boot protections. In order to load an untrusted or modified kernel, an attacker would first need to establish access to the system such as gaining physical access, obtain the ability to alter a pxe-boot network, or have remote access to a networked system with root access. With this access, an attacker could then craft a string to cause a buffer overflow by injecting a malicious payload that leads to arbitrary code execution within GRUB. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.

Cisco ASA Software and FTD Software Web Services Read-Only Path Traversal Vulnerability *(CVE-2020-3187, CVE-2020-3452)* Severity: **MEDIUM**

Description: A vulnerability in the web services interface of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to conduct directory traversal attacks and read sensitive files on a targeted system. The vulnerability is due to a lack of proper input validation of URLs in HTTP requests processed by an affected device. An attacker could exploit this vulnerability by sending a crafted HTTP request containing directory traversal character sequences to an affected device. A successful exploit could allow the attacker to view arbitrary files within the web services file system on the targeted device. The web services file system is enabled when the affected device is configured with either WebVPN or AnyConnect features.

Microsoft Windows Spoofing Vulnerability *(CVE-2020-1464)* Severity: **MEDIUM**

Description: A spoofing vulnerability exists when Windows incorrectly validates file signatures. An attacker who successfully exploited this vulnerability could bypass security features and load improperly signed files. In an attack scenario, an attacker could bypass security features intended to prevent improperly signed files from being loaded.

Google Chrome Arbitrary Code Execution Vulnerability *(CVE-2020-6519)* Severity: **MEDIUM**

Description: Policy bypass in CSP in Google Chrome allowed a remote attacker to bypass content security policy via a crafted HTML page. It could allow attackers to bypass the Content Security Policy (CSP) on websites, in order to steal data and execute rogue code.

Microsoft Sharepoint Server Remote Code Execution Vulnerability*(CVE-2020-1147)* Severity: **MEDIUM**

Description: A remote code execution vulnerability exists in .NET Framework, Microsoft SharePoint, and Visual Studio when the software fails to check the source markup of XML file input. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the process responsible for deserialization of the XML content.

Cisco DNA Center Information Disclosure Vulnerability *(CVE-2020-3411)* Severity: **MEDIUM**

Description:A vulnerability in Cisco DNA Center software could allow an unauthenticated remote attacker access to sensitive information on an affected system. The vulnerability is due to improper handling of authentication tokens by the affected software. An attacker could exploit this vulnerability by sending a

crafted HTTP request to an affected device. A successful exploit could allow the attacker access to sensitive device information, which includes configuration files.

Other Vulnerabilities

Cinterion Java Modules Vulnerability *(CVE-2020-15858)* Severity: **LOW**

Description: This security vulnerability could potentially allow attackers with physical access to the device to compromise certain assets stored in the Cinterion modules' flash file system such as: Customer Java MIDlet byte code, TLS credentials or OTAP configuration data.

Compiled with information from SANS' @RISK: The Concensus Security Vulnerability Alerts.

The Severity ratings on the above vulnerabilities are based on the NIST Common Vulnerability Scoring System Calculator (CVSS) version 2.0

For more information please contact us:

CERT Tonga
Ministry of MEIDECC
Nuku'alofa
Tel: 2378 (CERT)
email: cert@cert.gov.to
web: www.cert.gov.to
Twitter: @CERTTonga | Facebook: @CERTTonga