TLP: White[1]

Security Bulletin – July 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 Prime License Manager Privilege Escalation Vulnerability *(CVE-2020-3140)* Severity: HIGH

Description

A vulnerability in the web management interface of Cisco Prime License Manager (PLM) Software.

How it works

It could allow an unauthenticated, remote attacker to gain unauthorized access to an affected device. The vulnerability is due to insufficient validation of user input on the web management interface. An attacker could exploit this vulnerability by submitting a malicious request to an affected system.

What to do

Cisco has release the software updates that address the vulnerability.

Reference

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cisco-prime-priv-esc-HyhwdzBA

WinGate Privilege Escalation Vulnerability *(CVE-2020-13866)* Severity: HIGH

Description

WinGate has insecure permissions for the installation directory.

How it works

It allows local users ability to gain privileges by replacing an executable file with a Trojan horse. The WinGate directory hands full control to authenticated users, who can then run arbitrary code as SYSTEM after a WinGate restart or system reboot.

What to do

Always be sure to apply appropriate security updates recommended by WinGate

1 CERT Tonga adopts the Traffic Light Protocol

Reference

https://seclists.org/fulldisclosure/2020/Jun/11

SAP NetWeaver Application Server JAVA Multiple Vulnerabilities *(CVE-2020-6287)*

Severity: **HIGH**

Description

A vulnerability that can be exploited on SAP NetWeaver Application

How it works

SAP NetWeaver AS JAVA (LM Configuration Wizard) does not perform an authentication check which allows an attacker without prior authentication to execute configuration tasks to perform critical actions against the SAP Java system, including the ability to create an administrative user, and therefore compromising Confidentiality, Integrity and Availability of the system, leading to Missing Authentication Check.

What to do

Ensure to apply available security patches to prevent an adversary from exploiting this vulnerability

Reference

https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=552599675

F5 BIG-IP Remote Code Execution Vulnerability *(CVE-2020-5902)* Severity: **HIGH**

Description

F5 BIG-IP is exposed to remote code execution vulnerability.

How it works

The RECON (Remote Exploitable Code on NetWeaver) vulnerability that has been actively exploited in the wild. A successful exploit of RECON could give an unauthenticated attacker full access to the affected SAP system. This includes the ability to steal personally identifiable information from employees, customers and suppliers, corrupt data, delete or modify logs and traces. This can put organizations at risk.

What to do

F5 recommends that you install a fixed software version to fix this vulnerability.

Reference

https://support.f5.com/csp/article/K52145254

Citrix Application Delivery Controller and Gateway Directory Traversal Vulnerability

(CVE-2019-19781) Severity: **HIGH**

Description

An issue was discovered in Citrix Application Delivery Controller (ADC) and Gateway 10.5, 11.1, 12.0, 12.1, and 13.0. They allow Directory Traversal.

How it works

The vulnerability exists in Citrix Application Delivery Controller (ADC) formerly known as NetScaler ADC and Citrix Gateway formerly known as NetScaler Gateway that, if exploited, could allow an unauthenticated attacker to perform arbitrary code execution. This vulnerability exploits a directory traversal to execute an arbitrary command payload.

What to do

Citrix strongly urges affected to immediately upgrade to a fixed build OR apply the provided mitigation which applies equally to Citrix ADC, Citrix Gateway deployments.

Reference

https://support.citrix.com/article/CTX267027

Anchor Free OpenVPN SDK Privilege Escalation Vulnerability *(CVE-2020-12828)* Severity: HIGH

Description

An issue was discovered in Anchor Free VPN SDK.

How it works

The VPN SDK service takes certain executable locations over a socket bound to localhost. Binding to the socket and providing a path where a malicious executable file resides leads to executing the malicious executable file with SYSTEM privileges.

What to do

Ensure to apply appropriate security updates and patch as recommended by the Vendor

Reference

https://www.pango.co/sec31944/

Microsoft Windows SMBv3 Client/Server Remote Code Execution Vulnerability *(CVE-2020-0796)* Severity: HIGH

Description

A remote code execution vulnerability exists in the way that the Microsoft Server Message Block 3.1.1 (SMBv3) protocol handles certain requests.

How it works

An attacker who successfully exploited the vulnerability could gain the ability to execute code on the target server or client. To exploit the vulnerability against a server, an unauthenticated attacker could send a specially crafted packet to a targeted SMBv3 server.

What to do

Microsoft strongly recommends that you install the updates for this vulnerability as soon as they become available.

Also you can disable compression to block unauthenticated attackers from exploiting the vulnerability against an SMBv3 Server.

Reference

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0796

Palo Alto Networks PAN-OS Authentication Bypass in SAML Authentication Vulnerability

(CVE-2020-2021) Severity: **HIGH**

Description

A vulnerability in the Palo Alto Networks that could be exploited.

How it works

When Security Assertion Markup Language (SAML) authentication is enabled and the 'Validate Identity Provider Certificate' option is disabled (unchecked), improper verification of signatures in PAN-OS SAML authentication enables an unauthenticated network-based attacker to access protected resources.

What to do

Ensure that the signing certificate for your SAML Identity Provider is configured as the 'Identity Provider Certificate' before you upgrade to a fixed version to ensure that your users can continue to authenticate successfully.

Reference

https://security.paloaltonetworks.com/CVE-2020-2021

Microsoft LNK Remote Code Execution Vulnerability *(CVE-2020-1299, CVE-2020-1421)*

Severity: **HIGH**

Description

A remote code execution vulnerability exists in Microsoft Windows that could allow remote code execution if a .LNK file is processed.

How it works

The attacker could present to the user a removable drive, or remote share, that contains a malicious .LNK file and an associated malicious binary. When the user opens this drive(or remote share) in Windows Explorer, or any other application that parses the .LNK file, the malicious binary will execute code of the attacker’s choice, on the target system

What to do

Ensure to apply appropriate security updates as recommended by Microsoft

Reference

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1299

Microsoft Windows Defender Elevation of Privilege Vulnerability *(CVE-2020-1170)* Severity: **HIGH**

Description

An elevation of privilege vulnerability exists in Windows Defender that leads to arbitrary file deletion on the system.

How it works

To exploit the vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and take control of an affected system.

What to do

Apply appropriate security updates as recommended by Microsoft

Reference

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1170

Docker Desktop Privilege Escalation Vulnerability *(CVE-2020-10665)* Severity: **HIGH**

Description

A vulnerability that could be exploited in Docker Desktop

How it works

Docker Desktop allows local privilege escalation to NT AUTHORITY\SYSTEM because it mishandles the collection of diagnostics with Administrator privileges, leading to arbitrary DACL permissions overwrites and arbitrary file writes. This affects Docker Desktop Enterprise before 2.1.0.9, Docker Desktop for Windows Stable before 2.2.0.4, and Docker Desktop for Windows Edge before 2.2.2.0.

What to do

Apply appropriate security updates recommended by Docker Desktop

Reference

https://docs.docker.com/release-notes/

Other Vulnerabilities with known Exploits

Ruby On Rails Remote Code Execution Vulnerability*(CVE-2020-8163)* Severity: **MEDIUM**

Description: The is a code injection vulnerability that would allow an attacker who controlled the "locals" argument of a "render" call to perform a remote code execution vulnerability.

WordPress Theme NexosReal Estate 'search_order' SQL Injection Vulnerability*(CVE-2020-15363)* Severity: **MEDIUM**

Description: NexosReal Estate Theme is exposed to remote SQL injection vulnerability that allows side-map/?search_order= SQL Injection.

Oracle Java SE Critical Vulnerability *(CVE-2020-14664)* Severity: **MEDIUM**

Vulnerability in the Java SE product of Oracle Java SE (component: JavaFX). The supported version that is affected is Java SE: 8u251. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE.

VMware vCenter vmdir Information Disclosure Vulnerability *(CVE-2020-3952)* Severity: **MEDIUM**

Description: Under certain conditions vmdir does not correctly implement access controls. A malicious actor with network access to an affected vmdir deployment may be able to extract highly sensitive information which could be used to compromise vCenter Server or other services which are dependent upon vmdir for authentication.

Trend Micro Web Security Virtual Appliance Remote Code Execution Vulnerability*(CVE-2020-8605)* Severity: **MEDIUM**

Description: A vulnerability in Trend Micro InterScan Web Security Virtual Appliance may allow remote attackers to execute arbitrary code on affected installations. An attacker can leverage this vulnerability to disclose information in the context of the IWSS user. An authenticated remote attacker could exploit a command injection vulnerability in the product, leading to remote code execution

Apache Guacamole Information Disclosure Vulnerability*(CVE-2020-9497)* Severity: **MEDIUM**

Description: Apache Guacamole do not properly validate data received from RDP servers via static virtual channels. If a user connects to a malicious or compromised RDP server, specially-crafted PDUs could result in disclosure of information within the memory of the guard process handling the connection.

Microsoft Windows SMBv3 Client/Server Remote Code Execution Vulnerability*(CVE-2020-1206)* Severity: **MEDIUM**

Description: A format string vulnerability exists in AnyDesk that can be exploited for remote code execution. By sending a single UDP packet to the target machine, an attacker can successfully exploit the discovered format string vulnerability to gain Remote Code Execution.

Symantec Endpoint Protection Arbitrary file Write Vulnerability *(CVE-2020-5825* Severity: **MEDIUM**

Description: Symantec Endpoint Protection may be susceptible to an arbitrary file write vulnerability, which is a type of issue whereby an attacker is able to overwrite existing files on the resident system without proper privileges.

Other Vulnerabilities

Palo Alto Networks PAN-OS XML External Entity Reference Vulnerability *(CVE-2020-2012)*

Severity: **LOW**

Description: Improper restriction of XML external entity reference ('XXE') vulnerability in Palo Alto Networks Panorama management service allows remote unauthenticated attackers with network access to the Panorama management interface to read arbitrary files on the system.

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