CERT Tonga

Ministry of Meteorology Energy
Information, Disaster Management,
Environment, Communications and
Climate Change

TLP: White[1]

Security Bulletin – November 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

Oracle Solaris Remote Code Execution Vulnerability *(CVE-2020-14871)* Severity: **HIGH**

Description

A critical vulnerability exists in Oracle WebLogic Server product of Oracle Fusion Middleware (component: Console).

How it works

Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Solaris. While the vulnerability is in Oracle Solaris, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle Solaris.

What to do

Apply the appropriate security updates recommended by Oracle

Reference

https://www.oracle.com/security-alerts/cpuoct2020.html

VMware Horizon DaaS OpenSLP Remote Code Execution Vulnerability *(CVE-2020-9746)* Severity: **HIGH**

Description

OpenSLP as used in Horizon DaaS is exposed to heap overwrite issue.

How it works

A malicious actor with network access to port 427 on an ESXi host may be able to overwrite the heap of the OpenSLP service resulting in remote code execution.

What to do

Be sure to appropriate security updates recommended by vendor

[1] CERT Tonga adopts the Traffic Light Protocol

Reference

https://access.redhat.com/errata/RHSA-2020:0199

Git for Windows Large File Storage Remote Code Execution Vulnerability *(CVE-2020-27955)*

Severity: **HIGH**

Description

Git LFS 2.12.0 allows Remote Code Execution

How it works

On Windows, if Git LFS operates on a malicious repository with a git.bat or git.exe file in the current directory, that program is executed, permitting the attacker to execute arbitrary code. Successful exploitation allows attacker to execute remote code and compromise the system.

What to do

Apply the appropriate security updates recommended

Reference

https://legalhackers.com/advisories/Git-LFS-RCE-Exploit-CVE-2020-27955.html

Cisco Integrated Management Controller Multiple Remote Code Execution Vulnerabilities *(CVE-2020-3470)* Severity: **HIGH**

Description

Multiple vulnerabilities in the API subsystem of Cisco Integrated Management Controller (IMC)

How it works

A remote attacker could execute arbitrary code with root privileges. The vulnerabilities are due to improper boundary checks for certain user-supplied input. An attacker could exploit these vulnerabilities by sending a crafted HTTP request to the API subsystem of an affected system. When this request is processed, an exploitable buffer overflow condition may occur. A successful exploit could allow the attacker to execute arbitrary code with root privileges on the underlying operating system (OS)

What to do

Cisco has release the software updates that address the vulnerability.

Reference

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucs-api-rce-UXwpeDHd

Apache Struts Remote Code Execution Vulnerability *(CVE-2017-5638)* Severity: **HIGH**

Description

A vulnerability found on Apache

How it works

The Jakarta Multipart parser in Apache Struts has incorrect exception handling and error-message generation during file-upload attempts, which allows remote attackers to execute arbitrary commands via a crafted Content-Type, Content-Disposition, or Content-Length HTTP header, as exploited in the wild in March 2017 with a Content-Type header containing a #cmd= string.

What to do

Ensure that you apply the most appropriate updates recommended by Vendor

Reference

https://cwiki.apache.org/confluence/display/WW/S2-045

Citrix SD-WAN Center Remote Code Execution Vulnerability *(CVE-2020-8271)* Severity: HIGH

Description

Unauthenticated remote code execution with root privileges in Citrix SD-WAN Center versions before 11.2.2, 11.1.2b and 10.2.8

How it works

Multiple vulnerabilities have been discovered in Citrix SD-WAN Center that, if exploited, could allow an unauthenticated attacker with network access to SD-WAN Center to perform arbitrary code execution as root.

What to do

Apply the most appropriate security updates recommended by vendor

Reference

https://support.citrix.com/article/CTX285061

Microsoft Windows Kernel Privilege Escalation Vulnerability *(CVE-2020-17087)* Severity: HIGH

Description

A vulnerability found in Windows Kernal

What to do

Make sure to apply appropriate security updates recommended by Microsoft.

Reference

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17087

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.

How it works

The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. g engine handles objects in memory in Internet Explorer, aka 'Scripting Engine Memory Corruption Vulnerability'

What to do

Make sure to apply appropriate security updates recommended by Microsoft.

Reference

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

Microsoft Windows Kernel Elevation of Privilege Vulnerability *(CVE-2020-17087)* Severity: HIGH

Description

A remote code execution vulnerability Windows Kernel.

How it works

An attacker who successfully exploited the vulnerability could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

What to do

Ensure to apply appropriate security updates recommended by Microsoft.

Reference

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17087

Netlogon Elevation of Privilege Vulnerability *(CVE-2020-1472)* Severity: **HIGH**

Description

A vulnerability exists using the Netlogon Remote Protocol (MS-NRPC), aka 'Netlogon Elevation of Privilege Vulnerability'.

How it works

An elevation of privilege vulnerability exists when an attacker establishes a vulnerable Netlogon secure channel connection to a domain controller, using the Netlogon Remote Protocol (MS-NRPC), aka 'Netlogon Elevation of Privilege Vulnerability'

What to do

Apply the most appropriate security updates recommended by Microsoft.

Reference

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1472

Other Vulnerabilities with known Exploits

Google Chrome Freetype Heap Buffer Overflow Vulnerability *CVE-2020-15999*) Severity: **MEDIUM**

Description: Google Chrome issued an update announcement for the browser across all platforms. Google confirmed that the "stable channel" desktop Chrome browser is being updated across Windows, Mac, and Linux platforms. As per Google's official sources, this urgent update will start rolling out over the coming few days or weeks.

Apache Tomcat WebSocket Denial of Service Vulnerability *(CVE-2020-13935*) Severity: **MEDIUM**

Description: The payload length in a WebSocket frame was not correctly validated in Apache Tomcat. Invalid payload lengths could trigger an infinite loop. Multiple requests with invalid payload lengths could lead to a denial of service.

Apple iOS Memory Corruption Vulnerability *(CVE-2020-27930*) Severity: **MEDIUM**

Description: A memory corruption vulnerability exists in Apple iOS that may lead to arbitrary code execution when processing a maliciously crafted font. The vulnerability leads to memory corruption due to lack of proper input validation.

Drupal Core Remote Code Execution Vulnerability *(CVE-2020-13671*) Severity: **MEDIUM**

Description: Drupal core does not properly sanitize certain filenames on uploaded files, which can lead to files being interpreted as the incorrect extension and served as the wrong MIME type or executed as PHP for certain hosting configurations. Successful exploitation of these vulnerabilities could affect Confidentiality, Integrity and Availability.

Mozilla Firefox Arbitrary Local File Access Vulnerability *(CVE-2020-15647*) Severity: **MEDIUM**

Description: Description: A Content Provider in Firefox for Android allowed local files accessible by the browser to be read by a remote webpage, leading to sensitive data disclosure, including cookies for other origins.

Microsoft Windows TCP/IP Stack Remote Code Execution Vulnerability *(CVE-2020-16898*) Severity: **MEDIUM**

Description: A remote code execution vulnerability exists when the Windows TCP/IP stack improperly handles ICMPv6 Router Advertisement packets. An attacker who successfully exploited this vulnerability could gain the ability to execute code on the target server or client. To exploit this vulnerability, an attacker would have to send specially crafted ICMPv6 Router Advertisement packets to a remote Windows computer.

Fortinet FortiOS Directory Traversal Vulnerability *(CVE-2018-13379*) Severity: **MEDIUM**

Description: Fortinet FortiOS is exposed to a directory traversal vulnerability because it fails to properly sanitize user supplied input. A path traversal vulnerability in the FortiOS SSL VPN web portal may allow an unauthenticated attacker to download FortiOS system files through specially crafted HTTP resource requests.

Oracle Business Intelligence Unauthorized Access Vulnerability (*CVE-2020-14815)* Severity: **MEDIUM**

Description: A vulnerability exists in the Oracle Business Intelligence Enterprise Edition product of Oracle Fusion Middleware. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Business Intelligence Enterprise Edition. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Business Intelligence Enterprise Edition, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Business Intelligence Enterprise Edition accessible data as well as unauthorized update, insert or delete access to some of Oracle Business Intelligence Enterprise Edition accessible data.

Other Vulnerabilities

XStream Remote Code Execution Vulnerability *(CVE-2020-26217*)

Description: XStream is vulnerable to Remote Code Execution vulnerability that may allow a remote attacker to run arbitrary shell commands only by manipulating the processed input stream. Only users who rely on blocklists are affected.

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

Disclaimer Notice:

The information in this notice is intended solely for public knowledge and awareness, and not intending to harm, fright or disturb any person(s), legal entity or the receiver of this information. Under no circumstances shall the Ministry of MEIDECC be liable for any indirect, incidental, consequential, special or exemplary damages arising out of or in connection with your access or use of or inability to access or use the information and any third party content and services