CERT Tonga

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

TLP: White[1]

Security Bulletin – March 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

Microsoft Exchange Vulnerability (*CVE-2020-0688*) Severity: **HIGH**

An elevation of privilege vulnerability exists in the Windows Installer when MSI packages process symbolic links. An attacker who successfully exploited this vulnerability could bypass access restrictions to add or remove files.

How it works

The exploit first authenticates with the server through a POST /owa/auth.owa request. This POST request contains a valid username and password. After a successful authentication, the exploit requests the /ecp/default.aspx page in an attempt to get the content of __VIEWSTATEGENERATOR and the ASP.NET.SessionID. Using the data obtained from parsing the __VIEWSTATEGNERATOR, the exploit crafts a serialized payload containing the malicious command to be executed. The final serialized payload is then sent back to the /ecp/default.aspx.

What to do

- You can also read more about this on our previously issued Advisory on Micrsoft Exchange Vulnerability https://www.cert.gov.to/wp-content/uploads/2020/03/Advisory-Microsoft-Exchange-Vulnerability.pdf
- It is strongly advise users to upgrade to the most recent versions as soon as possible

Reference

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0688

[1] CERT Tonga adopts the Traffic Light Protocol

OpenBSD OpenSMTPD Local Privilege Escalation and Remote Code Execution Vulnerability

(*CVE-2020-8794*) Severity: **HIGH**

OpenSMTPD allows remote code execution because of an out-of-bounds read in mta_io in mta_session.c for multi-line replies.

How it works

A vulnerability has been discovered in OpenSMTPD which could allow for arbitrary code execution. An out of bounds read in smtpd allows an attacker to inject arbitrary commands into the envelope file which are then executed as root. Separately, missing privilege revocation in smtpctl allows arbitrary commands to be run with the _smtpq group. Successful exploitation of this vulnerability could allow an attacker to execute arbitrary code in the context of the server.

What to do

OpenBSD has released a patch in OpenSMTPD version 6.6.4p1 to address this vulnerability.

Reference

https://www.qualys.com/2020/02/24/cve-2020-8794/lpe-rce-opensmtpd-default-install.txt

D-Link DCH-M225 1.05b01 Vulnerability (*CVE-2020-6841*) Severity: **HIGH**

How it works

D-Link DCH-M225 1.05b01 and earlier devices allow remote attackers to execute arbitrary OS commands via shell metacharacters in the spotifyConnect.php userName parameter.

What to do

It is important for users, if you're using this product, that it has now reached End of Life(EoL) or End of Support(EoS) and there is no longer support or development for them.

Reference

https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10152

Cisco FXOS Software Vulnerability (*CVE-2020-3169*) Severity: **HIGH**

A vulnerability in the CLI of Cisco FXOS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying Linux operating system with a privilege level of root on an affected device**.**

How it works

The vulnerability is due to insufficient validation of arguments passed to a specific CLI command on the affected device. An attacker could exploit this vulnerability by including malicious input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system with root privileges. An attacker would need valid administrator credentials to exploit this vulnerability.

What to do

It is strongly advised to ensure that the devices to be upgraded contain sufficient memory and confirm that current hardware and software configurations will continue to be supported properly by the new release.

Reference

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20200226-fpwr-cmdinj

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

Microsoft has released a security advisory to address a remote code execution vulnerability in Microsoft Server Message Block 3.1.1 (SMBv3). SMB is a network file-sharing protocol that allows client machines to access files on servers.

Some of the major ransomware infections, has been the consequence of SMB-based exploits which was used in the WannaCry and NotPetya ransomware which spread globally through a worm-like behavior in 2017.

At the time of drafting this advisory, Microsoft had not release an update to patch this vulnerabilitiy. As such, constituents are encouraged to look out for this patch and update once it becomes available.

Please refer to our advisory for more: https://www.cert.gov.to/wp-content/uploads/2020/03/Advisory-Microsoft-SMBv3-Vulnerability.pdf

Reference

Microsoft- https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/adv200005

Microsoft Windows Background Intelligent Transfer Service Elevation of Privilege Vulnerability *(CVE 2020-0787)* Severity: **HIGH**

An elevation of privilege vulnerability exists when the Windows

Background Intelligent Transfer Service (BITS) improperly handles symbolic links. An attacker who successfully exploited this vulnerability could overwrite a targeted file leading to an elevated status.

How it works

To exploit this 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

It is advise for users of microsoft to apply the security updates as soon as possible

Reference

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0787

Apache Shardingsphere Vulnerability(CVE-2020-1947) Severity: **HIGH**

In Apache ShardingSphere(incubator) 4.0.0-RC3 and 4.0.0, the ShardingSphere's web console uses the SnakeYAML library for parsing YAML inputs to load datasource configuration.

How it works

SnakeYAML allows to unmarshal data to a Java type By using the YAML tag. Unmarshalling untrusted data can lead to security flaws of RCE.

What to do

It is highly recommended for users to upgrade software version to 4.0.1 or the latest

Reference

Apache:

- https://shardingsphere.apache.org/community/en/security/
- https://lists.apache.org/thread.html/r4a61a24c119bd820da6fb02100d286f8aae55c8f9b94a346b9bb27d8%40%3Cdev.shardingsphere.apache.org%3E

D-link -- dir-825 Vulnerability *(CVE-2020-10215)* Severity: **HIGH**

An issue was discovered on D-Link DIR-825 Rev.B 2.10 devices.

How it works

There is a stack-based buffer overflow in the httpd binary. It allows an authenticated user to execute arbitrary code via a POST to ntp_sync.cgi with a sufficiently long parameter ntp_server.

What to do

It is recommended to apply updated version from D-Link website and if it's no longer supported then please look out for the products that will be supported by the vendors to keep your devises up-to-date

Reference

https://github.com/kuc001/IoTFirmware/blob/master/D-Link/vulnerability4.md

Zyxel Remote Code Execution Vulnerability (CVE-2020-9054) Severity: **HIGH**

Multiple ZyXEL network-attached storage (NAS) devices running firmware contain a pre-authentication command injection vulnerability.

How it works

This allows an unauthenticated attacker to execute arbitrary code on a vulnerable device. ZyXEL NAS devices achieve authentication by using the weblogin.cgi CGI executable. This program fails to properly sanitize the username parameter that is passed to it. If the username parameter contains certain characters, it can allow command injection with the privileges of the web server that runs on the ZyXEL device.

What to do

It is strongly recommend that users follow the workaround procedure, as detailed below, to remediate the vulnerability.

Reference

https://www.zyxel.com/support/remote-code-execution-vulnerability-of-NAS-products.shtml

Joomla SQL Injection Vulnerability (CVE-2020-10243) Severity: **HIGH**

How it works

The lack of type casting of a variable in SQL statement leads to a SQL injection vulnerability in the "Featured Articles" frontend menutype.

What to do

It is strongly recommend that users to upgrade Joomla CMS version to 3.9.16 as soon as possible.

Reference

https://developer.joomla.org/security-centre/807-20200306-core-sql-injection-in-featured-articles-menu-parameters

VMware Fusion Privilege Escalation Vulnerability *(CVE-2020-3950)* Severity: **HIGH**

VMware Fusion, VMware Remote Console and Horizon Client for Mac contain a privilege escalation vulnerability due to improper use of setuid binaries.

How it works

Successful exploitation of this issue may allow attackers with normal user privileges to escalate their privileges to root on the system where Fusion, VMRC or Horizon Client is installed.

What to do

It is recommended to apply the updates recommended by the vendor and patch as soon as possible.

Reference

https://www.vmware.com/security/advisories/VMSA-2020-0005.html

Google Chrome Heap Corruption Vulnerability (*CVE-2020-6418*) Severity: **MEDIUM**

Type confusion in V8 in Google Chrome allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. Successful exploitation of this vulnerability could allow an attacker to execute arbitrary code in the context of the browser.

How it works

The exploit corrupts the length of a float array (float_rel), which can then be used for out of bounds read and write on adjacent memory. The relative read and write is then used to modify a UInt64Array (uint64_aarw) which is used for read and writing from absolute memory. The exploit then uses WebAssembly in order to allocate a region of RWX memory, which is then replaced with the payload shellcode. The payload is executed within the sandboxed renderer process, so the browser must be run with the --no-sandbox option for the payload to work correctly

What to do

It is advise for users who uses chrome browser to update with the stable version 80.0.3987.12

Reference

https://chromereleases.googleblog.com/2020/02/stable-channel-update-for-desktop_24.html

Microsoft Windows Security Feature Bypass Vulnerability *(CVE-2019-1019)* Severity: **MEDIUM**

A security feature bypass vulnerability exists where a NETLOGON message is able to obtain the session key and sign messages.

How it works

To exploit this vulnerability, an attacker could send a specially crafted authentication request. An attacker who successfully exploited this vulnerability could access another machine using the original user privileges.

What to do

It is strongly recommeded for users of Microsoft software and application to apply the security updates as soon a possible.

Reference

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1019

Other Vulneabilities with known Exploits

Apple MacOS Arbitrary File Overwrite Vulnerability *(CVE-2019-3830)* Severity: **MEDIUM**

Description: A validation issue existed in the handling of symlinks. This issue was addressed with improved validation of symlinks. A malicious application may be able to overwrite arbitrary files.

Windows Connected User Experiences and Telemetry Service Information Disclosure Vulnerability *(CVE-2020-0863)* Severity: **LOW**

Description: An information vulnerability exists when Windows Connected User Experiences and Telemetry Service improperly discloses file information. Successful exploitation of the vulnerability could allow the attacker to read any file on the file system. To exploit the vulnerability, an attacker would have to log onto an affected system and run a specially crafted application.

Google's Titan M chip Information Disclosure Vulnerability (*CVE-2019-9465*) Severity: **LOW**

Description: In the Titan M handling of cryptographic operations, there is a possible information disclosure due to an unusual root cause. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.

Other Vulnerabilities

WPA and WPA2 Disassociation Vulnerability ("Kr00k") (*CVE-2019-15126*) Severity: **LOW**

Description: An issue was discovered on Broadcom Wi-Fi client devices. Specifically timed and handcrafted traffic can cause internal errors (related to state transitions) in a WLAN device that lead to improper layer 2 Wi-Fi encryption with a consequent possibility of information disclosure over the air for a discrete set of traffic.

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).

Please for more information you can contact us:

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

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