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

TLP: White[1]

Security Bulletin – May 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

Google Android Bluetooth Remote Denial Of Service Vulnerability *(CVE-2020-0022)* Severity: HIGH

A remote denial of service vulnerability exists in Google Android.

How it works

In reassemble_and_dispatch of packet_fragmenter.cc, there is possible out of bounds write due to an incorrect bounds calculation. This could lead to remote code execution over Bluetooth with no additional execution privileges needed.

What to do

Apply appropriate updates by Google Android or mobile phone vendors to vulnerable systems.

Reference

https://source.android.com/security/bulletin/2020-02-01

Microsoft Windows Kernel Elevation of Privilege Vulnerability (*CVE-2018-8611)* Severity: HIGH

Microsoft Windows is prone to a local privilege-escalation vulnerability.

How it works

It fails to properly handle objects in memory, aka "Windows Kernel Elevation of Privilege Vulnerability. This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2019, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers.

What to do

Users of Microsoft software and application to apply the security updates as soon a possible.

[1] CERT Tonga adopts the Traffic Light Protocol

Reference

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8611

XG Firewall SQL injection Vulnerability (*CVE-2020-12271*) Severity: HIGH

A SQL injection issue exists on Sophos XG Firewall devices, as exploited in the wild in April 2020.

How it works

This affected devices configured with either the administration (HTTPS) service or the User Portal exposed on the WAN zone. A successful attack may have caused remote code execution that exfiltrated usernames and hashed passwords for the local device admin(s), portal admins, and user accounts used for remote access (but not external Active Directory or LDAP passwords)

What to do

It is strongly recommended for users to apply the security updates and to patch the vulnerability as soon a possible.

Reference

https://community.sophos.com/kb/en-us/135412

Microsoft Scripting Engine Memory Corruption Vulnerability *(CVE-2020-0674)* Severity: HIGH

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. 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.

The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit the vulnerability.

What to do

Users of Microsoft software and application are recommended to apply the security updates.

Reference

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0674

Oracle WebLogic Server T3 Protocol Deserialization of Untrusted Data Remote Code Execution Vulnerability (*CVE-2020-2883)* Severity:**HIGH**

Vulnerability found in the Oracle WebLogic Server product of Oracle Fusion Middleware.

How it works

Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3 to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server.

What to do

Ensure to apply the most appropriate security updates and patch as recommended by Oracle.

Reference

https://www.oracle.com/security-alerts/cpuapr2020.html#AppendixFMW

Pi-hole Remote Code Execution Vulnerability *(CVE-2020-11108)* Severity: **HIGH**

The Gravity updater in Pi-hole allows an authenticated adversary to upload arbitrary files. This can be abused for Remote Code Execution by writing to a PHP file in the web directory. The code error is in gravity_

How it works

This can be abused for Remote Code Execution by writing to a PHP file in the web directory. (Also, it can be used in conjunction with the sudo rule for the www-data user to escalate privileges to root.) The code error is in gravity_DownloadBlocklistFromUrl in gravity.sh

What to do

It is recommended to apply the security updates required by the vendor.

Reference

https://frichetten.com/blog/cve-2020-11108-pihole-rce/

Telerik Remote Code Execution Vulnerability (*CVE-2019-18935)* Severity:**HIGH**

Progress Telerik UI for ASP.NET AJAX through 2019.3.1023 contains a .NET deserialization vulnerability in the RadAsyncUpload function.

How it works

This is exploitable when the encryption keys are known due to the presence of CVE-2017-11317 or CVE-2017-11357, or other means. Exploitation can result in remote code execution. (As of 2020.1.114, a default setting prevents the exploit. In 2019.3.1023, but not earlier versions, a non-default setting can prevent exploitation.)

What to do

Ensure to apply the most appropriate security updates and patch as recommended by the vendors.

Reference

https://www.telerik.com/support/kb/aspnet-ajax/details/allows-javascriptserializer-deserialization

QNAP Pre-Auth Root Remote Code Execution Vulnerability*(CVE-2019-7192)* Severity: HIGH

QTS (QNAP Turbo NAS System) is a Turbo NAS Operating System, providing file storage, backup, disaster recovery, security management and virtualization applications for businesses; multimedia applications.

How it works

This improper access control vulnerability allows remote attackers to gain unauthorized access to the system.

What to do

To fix these vulnerabilities, it is recommended to update QTS and Photo Station to the latest version

Reference

https://www.qnap.com/zh-tw/security-advisory/nas-201911-25

vBulletin Remote SQL Injection Vulnerability *(CVE-2020-12720)*

Severity: **HIGH**

Security researchers discovered a vulnerability (CVE-2020-12720) in vBulletin Connect.

How it works

CVE-2020-12720 is an improper access control issue which could be exploited without prior authentication.

What to do

Patches available for the following versions of vBulletin Connect:

- 5.6.1 Patch Level 1
- 5.6.0 Patch Level 1
- 5.5.6 Patch Level 1

Users of vBulletin Cloud sites have already had the patch applied and do not need to take any action.

Reference

https://forum.vbulletin.com/forum/vbulletin-announcements/vbulletin-announcements_aa/4440032-vbulletin-5-5-6-5-6-0-5-6-1-security-patch-level-1

Apache Tomcat Remote Code Execution Vulnerability(*CVE-2020-9484)* Severity: **HIGH**

Apache Tomcat versions 7.0.0 through 7.0.103, 8.5.0 through 8.5.54, 9.0.0.M1 through 9.0.34 and 10.0.0-M1 through 10.0.0-M4 are susceptible to a vulnerability which when successfully exploited could lead to disclosure of sensitive information.

How it works

When using Apache Tomcat versions if

- a) an attacker is able to control the contents and name of a file on the server;
- b) the server is configured to use the PersistenceManager with a FileStore;
- c) the PersistenceManager is configured with sessionAttributeValueClassNameFilter="null" (the default unless a SecurityManager is used) or a sufficiently lax filter to allow the attacker provided object to be deserialized;
- d) the attacker knows the relative file path from the storage location used by FileStore to the file the attacker has control over; then, using a specifically crafted request, the attacker will be able to trigger remote code execution via deserialization of the file under their control. Note that all of conditions a) to d) must be true for the attack to succeed.

What to do

It is recommended that affected users upgrade Tomcat to the unaffected version as soon as possible

Reference

https://seclists.org/fulldisclosure/2020/Jun/6

https://security.netapp.com/advisory/ntap-20200528-0005/

Roundcube Vulnerability *(CVE-2020-12641)* Severity: **HIGH**

A vulnerability found in the Roundcube Webmail.

How it works

rcube_image.php in Roundcube Webmail before 1.4.4 allows attackers to execute arbitrary code via shell metacharacters in a configuration setting for im_convert_path or im_identify_path.

What to do

It is strongly recommended to update all productive installations of Roundcube with this new versions provided by the vendor.

Reference

https://roundcube.net/news/2020/04/29/security-updates-1.4.4-1.3.11-and-1.2.10

https://github.com/roundcube/roundcubemail/releases/tag/1.4.4

Vulnerability in the Quram qmg library of Samsung's Android OS *(CVE-2020-8899)* Severity: **HIGH**

There is a buffer overwrite vulnerability in the Quram qmg library of Samsung's Android OS versions O(8.x), P(9.0) and Q(10.0).

How it works

An unauthenticated, unauthorized attacker sending a specially crafted MMS to a vulnerable phone can trigger a heap-based buffer overflow in the Quram image codec leading to an arbitrary remote code execution (RCE) without any user interaction

What to do

It is strongly recommended to update Samsung Android OS to the latest version provided by the vendor.

Reference

https://security.samsungmobile.com/securityUpdate.smsb

https://bugs.chromium.org/p/project-zero/issues/detail?id=2002

Cisco Firepower Management Center Static Credential Vulnerabilities *(CVE-2020-3318)* Severity: **HIGH**

A vulnerability in Cisco FMC Software could allow an unauthenticated, remote attacker to access a sensitive part of an affected system with a high-privileged account.

How it works

This vulnerability is due to a system account that has a default and static password and that is not controlled by the system administrator. An attacker could exploit this vulnerability by using this default account to connect to the affected system. A successful exploit could allow the attacker to obtain *read* and *write* access to user agent data. The attacker would gain access to a sensitive portion of the system, but the attacker would not have full administrative rights to control the device.

What to do

Ensure that all devices are to be updated to the latest version required from Cisco.

Reference

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmcua-statcred-weeCcZct

Dell OS Recovery Image Insecure Inherited Permissions Vulnerability

(CVE-2020-5343) Severity: **HIGH**

Dell Windows 10 recovery images require an update to address an insecure inherited permissions vulnerability.

How it works

Dell Client platforms restored using a Dell OS recovery image downloaded before December 20, 2019, may contain an insecure inherited permissions vulnerability. A local authenticated malicious user with low privileges could exploit this vulnerability to gain unauthorized access on the root folder ice.

What to do

Vendor (Dell) recommends that all users apply the most appropriate updated version and take appropriate action.

Reference

https://www.dell.com/support/article/en-us/sln321036/dsa-2020-059-dell-os-recovery-image-insecure-inherited-permissions-vulnerability?lang=en

Google Android Elevation of Privilege Vulnerability *(CVE-2020-0096)* Severity: **HIGH**

Android is a mobile operating system based on a modified version of the Linux kernel and other open source software, designed primarily for touchscreen mobile devices such as smartphones and tablets.

How it works

In startActivities of ActivityStartController.java, there is a possible escalation of privilege due to a confused deputy. This could lead to local escalation of privilege with no additional execution privileges needed.

What to do

Ensure to apply appropriate updates by Google Android or mobile carriers to vulnerable systems

Reference

https://source.android.com/security/bulletin/2020-05-01

https://android.googlesource.com/platform/frameworks/base/+/a952197bd161ac0e03abc6acb5f48e4ec2a56e9d

Windows Print Spooler Elevation of Privilege Vulnerability *(CVE-2020-1048)* Severity: **HIGH**

An elevation of privilege vulnerability exists when the Windows Print Spooler service improperly allows arbitrary writing to the file system.

How it works

An attacker who successfully exploited this vulnerability could run arbitrary code with elevated system privileges. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted script or application.

What to do

Users of Microsoft software and application are recommended to apply the security updates.

Reference

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1048

Joomla Incorrect Access Control Vulnerability *(CVE-2020-11890)* Severity:**MEDIUM**

An issue was discovered in Joomla! before 3.9.17. Improper input validations in the usergroup table class could lead to a broken ACL configuration.

How it works

Multiple vulnerabilities have been identified in Joomla!. A remote user can exploit these vulnerabilities to trigger security restriction bypass and data manipulation on the targeted system.

What to do

Ensure to apply security updates for Joomla and upgrade to the latest version 3.9.17

Reference

https://developer.joomla.org/security-centre/810-20200402-core-missing-checks-for-the-root-usergroup-in-usergroup-table.html

Microsoft Win32k Elevation of Privilege Vulnerability *(CVE-2020-0624)* Severity: **MEDIUM**

An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory

How it works

An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode then exploit this vulnerability which could run arbitrary code in kernel mode then it install programs; view, change, or delete data; or create new accounts with full user rights.

What to do

Users of Microsoft software and application are recommended to apply the security updates.

Reference

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0624

Microsoft SharePoint Remote Code Execution Vulnerability (*CVE-2020-0932*) Severity: **MEDIUM**

A remote code execution vulnerability exists in Microsoft SharePoint when the software fails to check the source markup of an application package.

How it works

An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the SharePoint application pool and the SharePoint server farm account. Exploitation of this vulnerability requires that a user uploads a specially crafted SharePoint application package to an affected version of SharePoint.

What to do

Apply the appropriate security updates and patch by Microsoft.

Reference

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0932

Microsoft Windows Elevation of Privilege Vulnerability *(CVE-2020-0792)* Severity: **MEDIUM**

This vulnerability allows local attackers to escalate privileges on affected installations of Microsoft Windows. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.

How it works

The specific flaw exists within the function NtUserResolveDesktopForWOW. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a heap-based buffer. An attacker can leverage this vulnerability to escalate privileges and execute code in the context of SYSTEM.

What to do

Users of Microsoft software and application are recommended to apply the security updates.

Reference

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0792

Symantec Endpoint Protection Elevation of Privilege Vulnerability (*CVE-2020-5837)* Severity: **MEDIUM**

Symantec Endpoint Protection, prior to 14.3, may not respect file permissions when writing to log files that are replaced by symbolic links.

How it works

Symantec Endpoint Protection Manager could allow a local authenticated attacker to gain elevated privileges on the system, caused by an improper file permissions flaw when writing to log files that are replaced by symbolic links. By sending a specially-crafted request, an authenticated attacker could exploit this vulnerability to gain elevated privileges.

What to do

Apply the most appropriate update recommended patches by the vendor.

Reference

https://support.broadcom.com/security-advisory/security-advisory-detail.html?notificationId=SYMSA1762

https://labs.redyops.com/index.php/2020/04/27/symantec-endpoint-protection-sep-14-2-eop-via-arbitrary-write/

Other Vulnerabilities with known Exploits

FortiMail Authentication Bypass Vulnerability*(CVE-2020-9294)* Severity: **HIGH**

Description: An improper authentication vulnerability in FortiMail may allow a remote unauthenticated attacker to access the system as a legitimate user by requesting a password change via the user interface.

Saltstack Remote Code Execution Vulnerability*(CVE-2020-11651)* Severity: **HIGH**

Description: An issue was discovered in SaltStack Salt where, the salt-master process ClearFuncs class does not properly validate method calls. This allows a remote user to access some methods without authentication.

Zoho ManageEngine Arbitrary File Read Vulnerability*(CVE-2020-12116)* Severity: **MEDIUM**

Description: An issue was discovered in SaltStack Salt where, the salt-master process ClearFuncs class does not properly validate method calls. This allows a remote user to access some methods without authentication.

ISC BIND Denial of Service Vulnerability *(CVE-2020-8617)* Severity: **MEDIUM**

Description: Using a specially crafted message, an attacker may potentially cause a BIND server to reach an inconsistent state if the attacker knows (or successfully guesses) the name of a TSIG key used by the server. Since BIND, by default, configures a local session key even on servers whose configuration does not otherwise make use of it, almost all current BIND servers are vulnerable. A remote attacker could use this issue to cause Bind to crash, resulting in a denial of service, or possibly perform other attacks.

jQuery Cross Site Scripting Vulnerability *(CVE-2020-11022)* Severity: **MEDIUM**

Description: In jQuery, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. Successful exploitation of these vulnerabilities could lead to disclosure of sensitive information or addition or modification of data.

Other Vulnerabilities

Intel Wi-Fi Products Denial of Service Vulnerability *(CVE-2020-0558)* Severity: **LOW**

Description: Improper buffer restrictions in kernel mode driver for Intel PROSet/Wireless WiFi products on Windows 10 may allow an unprivileged user to potentially enable denial of service via adjacent access.

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).

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