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

TLP: White[1]

Security Bulletin – February 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 Excel Remote Code Execution Vulnerability (*CVE-2020-0759*) Severity: HIGH

A remote code execution vulnerability exists in Microsoft Excel software when the software fails to properly handle objects in memory. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the current user.

How it works

If the current user is logged on with administrative user rights, an attacker 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

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-2020-0759

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

1 CERT Tonga adopts the Traffic Light Protocol

How it works

An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. An attacker could then install programs; view, change, or delete data or create new accounts with full user rights.

What to do

It is highly recommended for upgrade to the most recent versions as soon as possible

Reference

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

Microsoft Windows kernel Elevation of Privilege Vulnerability *(CVE-2020-0683)* 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

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 add or remove files.

What to do

It is highly recommended to apply the most appropriate patch and update as soon as possible

Reference

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0683

Microsoft Active Directory Privilege Escalation Vulnerability *(CVE-2020-0665)* Severity:

MEDIUM

An elevation of privilege vulnerability exists in the way Active Directory handles information for domains in a transitively trusted forest

How it works

The attacker would first need to compromise a transitively trusted Active Directory forest.

An attacker who successfully exploited this vulnerability could obtain administrative rights on a computer in a domain which trusts the Active Directory forest under the attacker's control

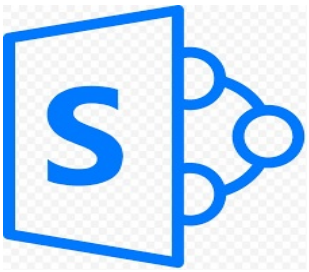
What to do

It is strongly advise users to upgrade to the latest version as soon as possible.

Reference

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0665

Microsoft SharePoint Remote Code Execution Vulnerability- (CVE-2020-0604) Severity- HIGH



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.

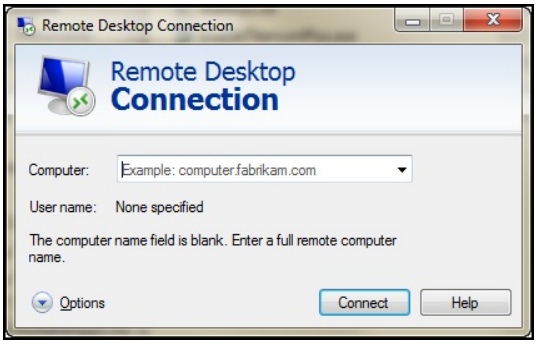
What to do

It is recommended to apply the most appropriate patch and update for the version as soon as possible.

Reference

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0604

Windows Remote Desktop Gateway (RD Gateway) Vulnerability- (CVE-2020-0609) Severity- HIGH



A remote code execution vulnerability exists in Windows Remote Desktop Gateway (RD Gateway) when an unauthenticated attacker connects to the target system using RDP and sends specially crafted requests.

How it works

This vulnerability is pre-authentication and requires no user interaction. An attacker who successfully exploited this vulnerability could execute arbitrary code on the target system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Also an attacker would need to send a specially crafted request to the target systems RD Gateway via RDP

What to do

It is strongly recommended to update software by enabling the Microsoft Updates and to ensure that you have the latest version.

Reference

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0609

OpenBSD OpenSMTPD Arbitrary Commands Execution Vulnerability *(CVE-2020-7247)*

Severity: **HIGH**

smtp_mailaddr in smtp_session.c in OpenSMTPD 6.6, as used in OpenBSD 6.6 and other products.

How it works

This allows remote attackers to execute arbitrary commands as root via a crafted SMTP session, as demonstrated by shell metacharacters in a MAIL FROM field. This affects the "uncommented" default configuration. The issue exists because of an incorrect return value upon failure of input validation.

What to do

OpenBSD has released a patch in OpenSMTPD version 6.6.2p1 to address this vulnerability.

Reference

https://www.openbsd.org/security.html

Apache Tomcat AJP File inclusion Vulnerability *(CVE-2020-1938)* Severity: **HIGH**

Apache Tomcat AJP file inclusion vulnerability allows an attacker to read any webapps files. If the Tomcat instance supports file uploads, the vulnerability could also be leveraged to achieve remote code execution.

How it works

It returns arbitrary files from anywhere in the web application including under the WEB-INF and META-INF directories or any other location reachable via ServletContext.getResourceAsStream() and processing any file in the web application as a JSP. Furthermore, if the web application allowed file upload and stored those files within the web application (or the attacker was able to control the content of the web application by some other means) then this, along with the ability to process a file as a JSP, made remote code execution possible.

What to do

It is highly recommended to update to the latest version of Apache Tomcat 9.0.31 or later

Reference

https://lists.apache.org/thread.html/r7c6f492fbd39af34a68681dbbba0468490ff1a97a1bd79c6a53610ef%40%3Cannounce.tomcat.apache.org%3E

Linux kernel vulnerability in the V4L2 subsystem (*CVE-2019-18683*) Severity: **HIGH**

An issue was discovered in drivers/media/platform/vivid in the Linux kernel through 5.3.8. It is exploitable for privilege escalation on some Linux distributions where local users have /dev/video0 access, but only if the driver happens to be loaded.

How it works

These issues are caused by wrong mutex locking in vivid_stop_generating_vid_cap(), vivid_stop_generating_vid_out(), sdr_cap_stop_streaming(), and the corresponding kthreads. At least one of these race conditions leads to a use-after-free.

What to do

It is strongly advised for users to upgrade to the most recent versions as soon as possible with the stable version 5.4.7

Reference

https://lore.kernel.org/lkml/20191103221719.27118-1-alex.popov@linux.com/

Adobe After Effects Out of Bounds Write Vulnerability (*CVE-2020- 3765*) Severity: **HIGH**

Adobe After Effects have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution.

How it Works

It allows attackers to execute arbitrary code in the context of current user running the affected application. Failed exploits will result in denial-of-service conditions.

What to do

It is strongly advise users to upgrade to the most recent versions as soon as possible with the latest version 5.4.7

Reference

https://helpx.adobe.com/security/products/after_effects/apsb20-09.html

Microsoft SQL Server Reporting Services Vulnerability *(CVE-2020-0618)* Severity- **MEDIUM**

A remote code execution vulnerability exists in Microsoft SQL Server Reporting Services when it incorrectly handles page requests.

How it works

To exploit the vulnerability, an authenticated attacker would need to submit a specially crafted page request to an affected Reporting Services instance

What to do

It is highly recommended to apply the most appropriate patch and update as soon as possible

Reference

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0618

Whatsapp Cross-Site Scripting Vulnerability (*CVE-2019-18426*) Severity: MEDIUM

A vulnerability in WhatsApp Desktop versions prior to 0.3.9309 when paired with WhatsApp for iPhone versions prior to 2.20.10

How it works

It allows cross-site scripting and local file reading. Exploiting the vulnerability requires the victim to click a link preview from a specially crafted text message.

What to do

It is strongly advise users to upgrade to the most recent versions as soon as possible

Reference

https://www.facebook.com/security/advisories/cve-2019-18426

Cisco IOS XR Software Intermediate System-to-Intermediate System Denial of Service Vulnerability *(CVE-2019-16027)* Severity: MEDIUM

A vulnerability in the implementation of the Intermediate System–to–Intermediate System (IS–IS) routing protocol functionality in Cisco IOS XR Software could allow an authenticated, remote attacker to cause a denial of service (DoS) condition in the IS–IS proces

How it works

The vulnerability is due to improper handling of a Simple Network Management Protocol (SNMP) request for specific Object Identifiers (OIDs) by the IS–IS process. An attacker could exploit this vulnerability by sending a crafted SNMP request to the affected device.

What to do

Cisco has released software updates that address this vulnerability, so please do update and patch with the most recent version

Reference

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20200122-ios-xr-dos

Other Vulneabilities with known Exploits

CORSAIR iCUE Driver Local Privilege Escalation Vulnerability *(CVE-2020-8808)* Severity: **HIGH**

Description: The CorsairLLAccess64.sys and CorsairLLAccess32.sys drivers in CORSAIR iCUE allows local non privileged users to read and write to arbitrary physical memory locations, and consequently gain NT AUTHORITY\SYSTEM privileges, via a function call such as MmMapIoSpace.

Tinywall Controller Privilege Escalation Vulnerability *(CVE-2019-19470)* – Severity: **HIGH**

Description: In Tinywall, unsafe usage of .NET deserialization in Named Pipe message processing allows privilege escalation to NT AUTHORITY\SYSTEM for a local attacker. An attacker who has already compromised the local system could use TinyWall Controller to gain additional privileges by attaching a debugger to the running process and modifying the code in memory.

Cacti authenticated Remote Code Execution Vulnerability *(CVE-2020-8813)* Severity: **HIGH**

Description: graph_realtime.php in Cacti allows remote attackers to execute arbitrary OS commands via shell metacharacters in a cookie, if a guest user has the graph real-time privilege. This vulnerability could be exploited without authentication if Cacti is enabling "Guest Realtime Graphs" privilege.

Pulse Secure Arbitrary File Disclosure Vulnerability (CVE-2019-11510) Severity: **HIGH**

Description: Pulse Connect Secure is exposed to arbitrary file disclosure vulnerability. An attacker can exploit these issues to access arbitrary files in the context of the application, write arbitrary files, or can send a specially crafted URI to perform an arbitrary file reading vulnerability

WordPress Code Snippets Plugin Remote Code Execution Vulnerability (CVE-2020-8417) Severity: **MEDIUM**

Description: WordPress plugin code snippets is vulnerable to cross site request forgery. Plugin's import function does not provide protection against CSRF. This vulnerability leads to Remote Code Execution. An attacker could possibly exploit this vulnerability and gain access to sensitive information.

Other Vulnerabilities

Vanilla Forums Security Bypass and Cookie Disclosure Vulnerabilities(*CVE-2011-3613, CVE-2011-3614*) Severity: **HIGH**

Description: Vanilla forums is exposed to an error within the handling of cookies that can be exploited to disclose cookie information. An error within the access control of the Facebook, Twitter, and Embed plugins can be used to bypass certain security restrictions.

ConnectWise Control User Enumeration Information Disclosure Vulnerability *(CVE-2019-16516)* Severity: **MEDIUM**

Description: An issue was discovered in ConnectWise Control (formerly known as ScreenConnect). ConnectWise Control is vulnerable to a user enumeration vulnerability, allowing an unauthenticated attacker to determine with certainty if an account exists for a given username.

Atlassian Jira Information Disclosure Vulnerability (*CVE-2019- 8449*) Severity: **MEDIUM**

Description: The /rest/api/latest/groupuserpicker resource in Jira before version 8.4.0 allows remote attackers to enumerate usernames via an information disclosure vulnerability.

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:

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