**TLP: White**[1]

# Security Bulletin – April 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

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

The vmdir is part of VMware's vCenter Server product, which provides centralized management of virtualized hosts and virtual machines (VMs) from a single console. VMware's Directory (vmdir) could lay bare the contents of entire corporate virtual infrastructures, if exploited by attackers it could allow them to bypass authentication mechanisms.

#### How it works

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.

#### What to do

Ensure to apply the security updates as soon a possible.

You can also read more about this on our previously issued Advisory on VMware Vulnerability https://www.cert.gov.to/wp-content/uploads/2020/04/Advisory-VMware-Vulnerability.pdf

#### Reference

https://www.vmware.com/security/advisories/VMSA-2020-0006.html

### Google Android Privilege Escalation Vulnerability (*CVE-2020-0041*) Severity: HIGH

In binder_transaction of binder.c, there is a possible out of bounds write due to an incorrect bounds check.

1 CERT Tonga adopts the Traffic Light Protocol

**How it works**

This could lead to local escalation of privilege with no additional execution privileges needed with no user interaction needed for this exploitation.

**What to do**

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

**Reference**

https://source.android.com/security/bulletin/2020-03-01

## Apple MacOS Privilege Escalation Vulnerability (*CVE-2020-3919*) Severity: **HIGH**

The vulnerability was caused by a logic error when computing the number of valid offsets that have already been validated by the driver.

In particular, when the binder driver is processing a transaction it walks through a number of offsets and validates and translates binder objects at each such offset.

**How it works**

A malicious application may be able to execute arbitrary code with kernel privileges.

**What to do**

Ensure that software and application for Apple OS is being updated to the latest version.

**Reference**

https://support.apple.com/en-us/HT211100

https://labs.bluefrostsecurity.de/blog/2020/03/31/cve-2020-0041-part-1-sandbox-escape/

## VMWare Workstation vmnetdhcp Denial of Service Vulnerability *(CVE-2020-3947)* Severity: **HIGH**

VMware Workstation contain a use-after vulnerability in vmnetdhcp. file it is a software component of VMware Workstation. VMware provides the ability to run virtual workstations within another operating system. vmnetdhcp provides the means of DHCP communication between the client VM and the host operating system.

**How it works**

Successful exploitation of this issue may lead to code execution on the host from the guest or may allow attackers to create a denial of service condition of the vmnetdhcp service running on the host machine.

**What to do**

It is advised to apply the appropriate security patch and updates recommended by the vendor.

### Reference

https://www.vmware.com/security/advisories/VMSA-2020-0004.html

## Oracle Coherence Remote Code Execution Vulnerability *(CVE-2020-2555)* Severity: **HIGH**

A vulnerability exists in the Oracle Coherence product of Oracle Fusion Middleware.

### How it works

Easily exploitable vulnerability by allowing unauthenticated attacker with network access via T3 to compromise Oracle Coherence. Successful attacks of this vulnerability can result in takeover of Oracle Coherence.

### What to do

Users are to apply the security updates and patch available as soon a possible.

### Reference

https://www.oracle.com/security-alerts/cpujan2020.html#AppendixFMW

## OpenSSL Denial of service Vulnerability *( CVE-2020-1967 )* Severity: **HIGH**

Server or client applications that call the SSL_check_chain() function during or after a TLS 1.3 handshake may crash due to a NULL pointer dereference as a result of incorrect handling of the "signature_algorithms_cert" TLS extension.

### How it works

The crash occurs if an invalid or unrecognised signature algorithm is received from the peer. This could be exploited by a malicious peer in a Denial of Service attack. OpenSSL version 1.1.1d, 1.1.1e, and 1.1.1f are affected by this issue. This issue did not affect OpenSSL versions prior to 1.1.1d. Fixed in OpenSSL 1.1.1g (Affected 1.1.1d-1.1.1f).

### What to do

This issue has not affect OpenSSL 1.1.0 however this version is out of support and no longer receiving updates. So users of this versions should upgrade to OpenSSL 1.1.1.

### Reference

https://www.openssl.org/news/secadv/20200421.txt

## Linux Kernel Privilege Escalation Vulnerability *(CVE-2020-8835)* Severity:**HIGH**

A Vulnerability discovered that the bpf verifier in the Linux kernel did not properly calculate register bounds for certain operations.

### How it works

In the Linux kernel 5.5.0 and newer, the bpf verifier (kernel/bpf/verifier.c) did not properly restrict the register bounds for 32-bit operations, leading to out-of-bounds reads and writes in kernel memory. The vulnerability also affects the Linux 5.4 stable series, starting with v5.4.7, as the introducing commit was backported to that branch.

### What to do

Apply the security updates as well as the latest version as soon a possible.

### Reference

https://git.kernel.org/pub/scm/linux/kernel/git/netdev/net-next.git/commit/?id=f2d67fec0b43edce8c416101cdc52e71145b5fef

https://lore.kernel.org/bpf/20200330160324.15259-1-daniel@iogearbox.net/T/

## Zoho ManageEngine Desktop Central Remote Code Execution Vulnerability *( CVE-2020 10189 )* Severity: **HIGH**


A vulnerability was discovered in Zoho ManageEngine Desktop Central. Remote code execution because of deserialization of untrusted data in getChartImage in the FileStorage class. System.

### How it works

This is related to the CewolfServlet and MDMLogUploaderServlet servlets. An attacker could exploit this vulnerability to escalate privilege on the target.

### What to do

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

### Reference

https://srcincite.io/advisories/src-2020-0011/

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


A remote code execution vulnerability that exists in the way the scripting engine handles objects in memory in Internet Explorer. Exploitation of this vulnerability could allow an attacker to corrupt memory and execute arbitrary code with the same level of privileges as the current user.

### How it works

To exploit this vulnerability an attacker would be required to host a maliciously crafted website designed to take advantage of this Internet Explorer vulnerability and then require a target to visit the website. A target could be convinced to visit the website via social engineering by embedding a link to it in an email, compromising a legitimate website or forum, or alternatively the link could be embedded in a file that

supports the execution of scripts when opened, such as Microsoft Office Documents, PDF files, or HTML files.

**What to do**

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-2020-0674

### Microsoft Windows Kernel Elevation of Privilege Vulnerability (CVE-2020-1027) Severity: HIGH

An elevation of privilege vulnerability exists in the way that the Windows Kernel handles objects in memory.

**How it works**

An attacker who successfully exploited the vulnerability could execute code with elevated permissions. To exploit the vulnerability, a locally authenticated attacker could run a specially crafted application.

**What to do**

It is strongly recommended 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-2020-1027

### Microsoft Graphics Remote Code Execution Vulnerability *(CVE-2020-0687)* Severity:HIGH

A remote code execution vulnerability exists when the Windows font library

**How it works**

It improperly handles specially crafted embedded fonts and so an attacker who successfully exploited the vulnerability could take control of the affected system.

**What to do**

Be sure to apply security updates  for Microsoft application as soon a possible with the latest updates

**Reference**

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0687

### Microsoft Adobe Font Manager Library Remote Code Execution Vulnerability *(CVE-2020-1020)* Severity: MEDIUM

A remote code execution vulnerability exists in Microsoft Windows when the Windows Adobe Type Manager Library

**How it works**

It improperly handles a specially-crafted multi-master font - Adobe Type 1 PostScript format.

**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-2020-1020

## Microsoft Media Foundation Information Disclosure Vulnerability (*CVE-2020-0939)*

Severity:**MEDIUM**

An information disclosure vulnerability exists when Media Foundation

**How it works**

It improperly handles objects in memory which an attacker who successfully exploited this vulnerability could obtain information to further compromise the user's system.

**What to do**

Ensure users of Microsoft software and application applies the appropriate security updates and patch.

**Reference**

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0939

## Microsoft Windows Kernel Elevation of Privilege Vulnerability (CVE-2020-0760) Severity:

**MEDIUM**

A remote code execution vulnerability exists when Microsoft Office improperly loads arbitrary type libraries.

**How it works**

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.

To exploit the vulnerability, an attacker must first convince a user to open a specially crafted Office document

**What to do**

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

**Reference**

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0760

### PHP Information Disclosure Vulnerability *( CVE-2020-7066)* Severity: **MEDIUM**

A vulnerability discovered in the PHP, get_headers() silently truncates anything after a null byte in the URL it uses

**How it works**

PHP versions 7.2.x below 7.2.9, 7.3.x below 7.3.16 and 7.4.x below 7.4.34, while using get_headers() with user-supplied URL, if the URL contains zero (\0) character, the URL will be silently truncated at it. This may cause some software to make incorrect assumptions about the target of the get_headers() and possibly send some information to a wrong server.

**What to do**

Be sure to apply the security updates for the following software and application with the latest version.

**Reference**

https://bugs.php.net/bug.php?id=79329

### Sudo Buffer Overflow Vulnerability (*CVE-2019-18634*) Severity: **MEDIUM**


In Sudo versions, if pwfeedback is enabled in /etc/sudoers, users can trigger a stack-based buffer overflow in the privileged sudo process.

**How it works**

(pwfeedback is a default setting in Linux Mint and elementary OS; however, it is NOT the default for upstream and many other packages, and would exist only if enabled by an administrator.) The attacker needs to deliver a long string to the stdin of getln() in tgetpass.c.

**What to do**

Do make sure that the software and application is being updated to the latest version.

**Reference**

https://www.sudo.ws/security.html

## Other Vulneabilities with known Exploits

### OpenWrt's opkg Man In The Middle Attack Vulnerability *(CVE-2020-7982)* Severity: **HIGH**

Description: A bug in the fork of the opkg package manager before 2020-01-25 prevents correct parsing of embedded checksums in the signed repository index, allowing a man-in-the-middle attacker to inject arbitrary package payloads (which are installed without verification).

### DrayTek pre-auth Remote Code Execution Vulnerability *(CVE-2020-8515)* Severity: **HIGH**

Description: DrayTek devices allow remote code execution as root (without authentication) via shell metacharacters to the cgi-bin/mainfunction.cgi URI.

**Sonatype Nexus Repository Remote Code Execution Vulnerability** *(CVE-2020-10204)* Severity: **HIGH**

Description: A Remote Code Execution vulnerability has been discovered in Nexus Repository Manager requiring immediate action. The vulnerability allows for an attacker with any type of account on NXRM to execute arbitrary code by crafting a malicious request to NXRM.

## Other Vulnerabilities

**HAPaproxy hpack-tbl.c Out of Bounds Write Vulnerability** (CVE-2020-0760) Severity: **MEDIUM**

Description: A vulnerability exists in hpack-tbl.c present in the HPACK decoder in HAProxy, wherein a remote attacker can write arbitrary bytes around a certain location on the heap via a crafted HTTP/2 request, possibly causing remote code execution. This vulnerability could be exploited to gain access to sensitive information also use this vulnerability to change contents or configuration on the system. Additionally, this vulnerability can also be used to cause a denial of service in the form of interruptions in resource availability.

**Zyxel Cross Site Scripting Vulnerability** (CVE-2019-13495) Severity: **LOW**

Description: In firmware version of Zyxel XGS2210-52HP, multiple stored cross-site scripting (XSS) issues allows remote authenticated users to inject arbitrary web script via an rpSys.html Name or Location field.

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