TLP: White[1]

Security Bulletin - July 2019

Dear Constituents,

Welcome to the Security Bulletin for July 2019.

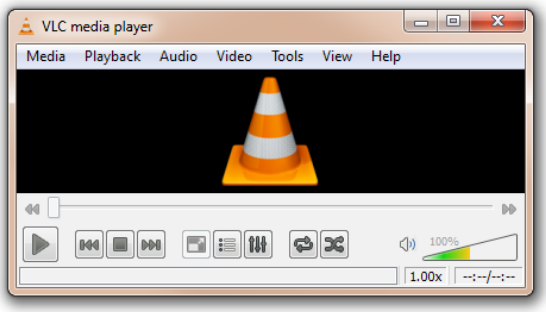
On our security bulletins, we will try and compile list of vulnerabilities, especially those with known exploits in the wild during the month that we think that are relevant to Tonga.

As always, we welcome your comments and feedback and if you can please forward them to cert@cert.gov.to

Vulnerabilities with Active Exploits in the Wild

VideoLAN VLC Heap Based Buffer Overflow Vulnerability *(CVE-2019-13962)*

A vulnerability in VideoLAN VLC media player could allow a local attacker to execute arbitrary code or cause a denial of service (DoS) condition on a targeted system.



How it works

The vulnerability is due to a heap-based buffer overflow condition that exists in the *mkv::demux_sys_t::FreeUnused* function, as defined in the *modules/demux/mkv/demux.cpp* source code file of the affected software.

- An attacker could exploit this vulnerability by making a malicious request on the targeted system.
- A successful exploit could allow the attacker to execute arbitrary code or cause a DoS condition on the targeted system.

What to do

Update your VLC to the latest version.

Reference

- **VideoLAN Client**: https://trac.videolan.org/vlc/ticket/22474

1 CERT Tonga adopts the Traffic Light Protocol

Apache HTTP Server Local Privilege Escalation Vulnerability *(CVE-2019-0211)*

Apache is the most widely used web server software running on 67% of all webservers in the world. Apache is a free, open-source software utilized by individuals and corporations on a global scale. Given the high utilization of Apache, a malicious script that could override permissions on Apache web server puts all systems vulnerable.

How it works

A flaw has been discovered in Apache which allows for local privilege escalation where a person or program that has limited access or privileges (such as a user account) may be able execute code with root privileges.

Apache HTTP Server 2.4 releases 2.4.17 to 2.4.38, with MPM event, worker or prefork, code executing in less-privileged child processes or threads (including scripts executed by an in-process scripting interpreter) could execute arbitrary code with the privileges of the parent process (usually root) by manipulating the scoreboard.

What to do

Make sure to update your Apache web server to the latest version

Reference

- **Apache**: https://httpd.apache.org/security/vulnerabilities_24.html#CVE-2019-0211

D-Link DIR-818LW Multiple Command Injection Vulnerabilities *(CVE-2019-13482)*

A flaw was recently discovered on D-Link DIR-818LW devices with firmware 2.06betab01.

How it works

Exploiting these vulnerabilities could allow an attacker to execute arbitrary commands in the context of the affected device. There is a command injection in HNAP1 (exploitable with Authentication) via shell metacharacters in the MTU field to SetWanSettings.

Failed exploit attempts will likely result in denial-of-service conditions. D-Link DIR-818LW devices with firmware 2.06betab01 are vulnerable.

What to do

Making sure that you update the firmware version of D-Link to the latest.

Reference

- https://github.com/TeamSeri0us/pocs/blob/master/iot/dlink/dir818-3.pdf
- https://github.com/TeamSeri0us/pocs/blob/master/iot/dlink/dir818-4.pdf

Linux kernel Local Privilege Escalation Vulnerability *(CVE-2019-12817)*

Linux Kernel is prone to a local privilege-escalation vulnerability. A local attacker can exploit this issue to gain elevated privileges.

How it works

It was discovered that the Linux kernel did not properly separate certain memory mappings when creating new userspace processes on 64-bit Power (ppc64el) systems. A local attacker could use this to access memory contents or cause memory corruption of other processes on the system.

- arch/powerpc/mm/mmu_context_book3s64.c in the Linux kernel before 5.1.15for powerpc has a bug where unrelated processes may be able to read/writeto one another's virtual memory under certain conditions via an mmap above 512 TB.

What to do

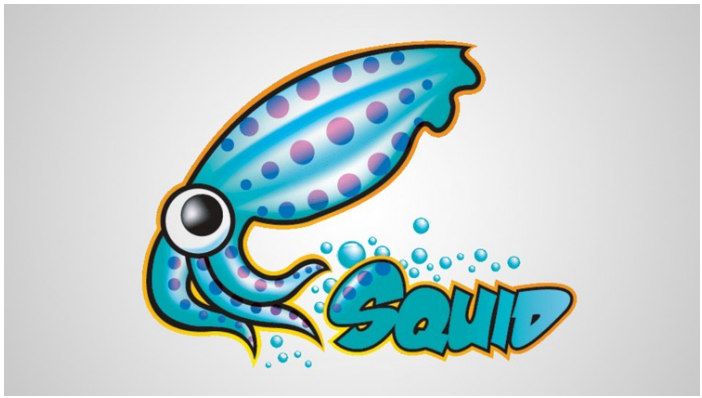
Please be sure update packages for linux to the latest version

Reference

Ubuntu: https://usn.ubuntu.com/4031-1/

Squid Multiple Cross Site Scripting Vulnerabilities *(CVE-2019-13345)*

Squid is a cache and proxy server based on Unix. It is exposed to multiple cross site scripting (XSS) vulnerabilities because it fails to sanitize user-supplied input.



How it works

An attacker may leverage these issues to execute arbitrary script code in the browser of an unsuspecting user in the context of the affected site. This may allow the attacker to steal cookie based authentication credentials and launch other attacks.

What to do

Update squid to the latest version 4.8

Reference

- **Squid Proxy Cache Security Update Advisory SQUID-2019:6 -** http://squid-web-proxy-cache.1019090.n4.nabble.com/squid-announce-ADVISORY-SQUID-2019-6-Multiple-Cross-Site-Scripting-issues-in-cachemgr-cgi-td4687960.html

Vulnerabilities in Zoom meeting software could turn on Mac cameras *(CVE-2019-13449 and CVE-2019-13450)*

Two vulnerabilities in the Zoom remote could allow an attacker to use a malicious website to automatically start a Zoom meeting and look in on a user's Mac camera.

How it works

- This vulnerability allows any website to forcibly join a user to a Zoom call, with their video camera activated, without the user's permission.
- On top of this, this vulnerability would have allowed any webpage to DOS (Denial of Service) a Mac by repeatedly joining a user to an invalid call.
- Additionally, if you've ever installed the Zoom client and then uninstalled it, you still have a localhost web server on your machine that will happily re-install the Zoom client for you, without requiring any user interaction on your behalf besides visiting a webpage

What to do

Users are encouraged to ensure the Mac Zoom app is up to date and to disable the setting that allows Zoom to automatically turn on the machine's camera when joining a meeting.

Reference

Infosec Write Up: https://medium.com/bugbountywriteup/zoom-zero-day-4-million-webcams-maybe-an-rce-just-get-them-to-visit-your-website-ac75c83f4ef5

Other Vulneabilities with known exploits

Oracle WebLogic Server Deserialization RCE Vulnerability (*CVE-2019-2725)*

Oracle WebLogic Server is exposed to a remote command execution vulnerability. Attackers can exploit this issue to execute an arbitrary command within the context of a user running the affected application. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server.

Palo Alto Networks PAN-OS Multiple Remote Code Execution Vulnerabilities *(CVE-2019-1579)*

Palo Alto Networks PAN-OS is exposed to multiple remote code execution vulnerabilities. Remote Code Execution in PAN-OS with GlobalProtect Portal or GlobalProtect Gateway Interface enabled may allow an unauthenticated remote attacker to execute arbitrary code. Successfully exploiting these issues may result in the execution of arbitrary code in the context of the affected application.

OWASP AntiSamy Cross Site Scripting Vulnerability *(CVE-2017-14735)*

OWASP AntiSamy is exposed to a cross site scripting vulnerability because it fails to properly sanitize user supplied input. An attacker may leverage this issue to execute arbitrary script code in the browser of an unsuspecting user in the context of the affected site. This may let the attacker steal cookie-based authentication credentials and launch other attacks

Apache Roller Cross Site Scripting Vulnerability *(CVE-2019-0234)*

Apache Roller is exposed to a cross site scripting vulnerability because it fails to properly sanitize user-supplied input. A Reflected Cross site Scripting vulnerability exists in Apache Roller. Roller's Math Comment Authenticator did not property sanitize user input and could be exploited to perform Reflected Cross Site Scripting. An attacker may leverage this issue to execute arbitrary script code in the browser of an unsuspecting user in the context of the affected site.

Nessus Cross Site Scripting Vulnerability *(CVE-2019-3961)*

Nessus is exposed to a cross site scripting vulnerability because it fails to properly sanitize user supplied input. An unauthenticated, remote attacker could potentially exploit this vulnerability via a specially crafted request to execute arbitrary script code in a users browser session. An attacker may leverage this issue to execute arbitrary script code in the browser of an unsuspecting user in the context of the affected site. This may allow the attacker to steal cookie based authentication credentials and launch other attacks.

GitLab Cross Site Scripting Vulnerability (CVE-2018-19570)

GitLab is exposed to a cross site scripting vulnerability because it fails to properly sanitize user-supplied input. An attacker may leverage this issue to execute arbitrary script code in the browser of an unsuspecting user in the context of the affected site. Fields that accept Markdown contained incomplete input validation and output encoding when accepting unrecognized HTML tags, which resulted in a persistent cross site scripting vulnerability.

ImageMagick Multiple Security Vulnerabilities *(CVE-2019-12974)*

A NULL pointer dereference in the function ReadPANGOImage in coders/pango.c and the function ReadVIDImage in coders/vid.c in ImageMagick allows remote attackers to cause a denial of service via a crafted image. Successfully exploiting these issues may allow an attacker to gain access to sensitive information, bypass certain security restrictions and to perform unauthorized actions or cause a denial of service condition. This may aid in launching further attacks.

Philips Holter Local Security Bypass Vulnerability *(CVE-2019-10968)*

Philips Holter is exposed to a local security bypass vulnerability. A local attacker can exploit this issue to bypass security restrictions and gain unauthorized access to the disabled features of the product.

LiveZilla Server SQL Injection Vulnerability *(CVE-2019-12939)*

LiveZilla Server is exposed to an SQL injection vulnerability because it fails to sufficiently sanitize user-supplied data before using it in an SQL query. An attacker may leverage this issue to compromise the application, access or modify data, or exploit latent vulnerabilities in the underlying database.

Other Vulnerabilities

- **Firefox patches critical zero-day used to target Macs**

A type confusion vulnerability can occur when manipulating JavaScript objects due to issues in `Array.pop`. This can allow for an exploitable crash. We are aware of targeted attacks in the wild abusing this flaw.

- **Anubis malware returns to haunt Android users**

Researchers at Trend Micro recently discovered more than 17,400 new samples of the Android malware. Anubis has targeted several different banking apps on Android stores, installing malicious espionage and banking trojan capabilities onto users' mobile devices. The actor behind Anubis has been active for at least 12 years, constantly making updates and adding new features. All four of these rules fire when Anubis attempts to make an outbound connection to a command and control (C2) server.

- **Unpatched flaw in LibreOffice allows Malicious Code Execution**

LibreOffice is one of the most popular and open source alternatives to Microsoft Office suite and is available for Windows, Linux and macOS systems. It contains a severe unpatched code execution vulnerability that could sneak malware into your system as soon as you open a maliciously-crafted document file.

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