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

TLP: White[1]

Security Bulletin – November 2019

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 Chrome Use-After-Free Vulnerability (*CVE-2019-13720*) Severity: HIGH

Google is warning users of a high-severity vulnerability in its Chrome browser that is currently being exploited by attackers to hijack computers.

How it works

It is a use-after-free flaw, which is a memory corruption flaw where an attempt is made to access memory after it has been freed. This can cause an array of malicious impacts, from causing a program to crash, to potentially leading to execution of arbitrary code – or even enable full remote code execution capabilities.

What to do

Google is urging users to update to the latest version of Chrome, 78.0.3904.87 or later (for Windows, Mac, and Linux)

Reference:

https://chromereleases.googleblog.com/2019/10/stable-channel-update-for-desktop_31.html

Whatsapp Remote Code Execution Vulnerability (*CVE-2019-11932*) Severity: HIGH

A researcher has released details of a WhatsApp flaw that could be used to compromise the app and the mobile device the app is running on.

1 CERT Tonga adopts the Traffic Light Protocol

How it works

The researcher says an attack would involve first sending a malicious GIF image using any channel, that is by email, a rival messaging app, or sent direct through WhatsApp itself.

If WhatsApp is being used, and the attacker (or hapless intermediary) is on the contacts list of the user as a friend, apparently this GIF would download to the device automatically.

Execution would happen when the recipient subsequently opens the WhatsApp Gallery even if no file is selected or sent.

What to do

Android versions 8.1 and 9.0 are exploitable, but older versions of the operating system -- Android 8.0 and below -- are not. The researcher says that the double-free bug could still be triggered, but in older OS versions, a crash occurs before any malicious code can be executed to tamper with chat sessions.

Facebook has acknowledged the security issue and has patched the problem in WhatsApp version 2.19.244 so are adviced to please update to the latest version.

Reference:

https://awakened1712.github.io/hacking/hacking-whatsapp-gif-rce/

PHP 7 Remote Code Execution Vulnerability (*CVE-2019-11043*) Severity: **HIGH**

A buffer underflow bug in PHP could allow remote code-execution (RCE) on targeted NGINX servers

How it works

This vulnerability has been rated critical since the exploit is considered simple, achieves persistence once abused, is limited to affecting a certain type of configurations, and authentication is not required. It can allow hackers and threat actors to take over a PHP-written or -supported web application and its web server. This allows attackers to steal, delete, add, or overwrite content, embed them with malware, or use them as doorways into other systems or servers connected to it.

PHP is the framework for many popular websites and web applications, including content management systems WordPress and Drupal

What to do

IT teams using NGINX with PHP-FPM are recommended to update their PHP to their latest or stable versions (7.2.24 or 7.3.11), which have addressed the vulnerability along with other bugs. If the patch or upgrade is not feasible or cannot be immediately applied a workaround is provided by adding rules to check if a file exists or not, or filters in URLs

Reference:

https://github.com/neex/phuip-fpizdam

SUDO Security Policy Bypass Vulnerability (*CVE-2019-14287*) Severity: **HIGH**

A vulnerability has been discovered in Sudo—one of the most important, powerful utilities that comes as a core command installed on almost every UNIX and Linux-based operating system. The vulnerability in question is a sudo security policy bypass issue that could allow a malicious user or a program to execute arbitrary commands as root even when the "sudoers configuration" explicitly disallows the root access

How it works

In Sudo before 1.8.28, an attacker with access to a Runas ALL sudoer account can bypass certain policy blacklists and session PAM modules, and can cause incorrect logging, by invoking sudo with a crafted user ID. For example, this allows bypass of !root configuration, and USER= logging, for a "sudo -u \#$ ((0xffffffff))" command.

What to do

Users are highly recommended to update sudo package to the latest version as soon as it is available.

Reference:

https://www.sudo.ws/alerts/minus_1_uid.html

D-Link Unauthenticated Remote Code Execution Vulnerability (*CVE-2019-16920*) Severity: **HIGH**

D-LINK DIR-655

D-LINK DIR-866L

D-LINK DIR-652

D-LINK DHP-1565

Security researchers disclosed a new unauthenticated command injection vulnerability in some of the D-link routers in which if successfully exploited results in Remote Code Execution, an attacker can trigger the vulnerability remotely to access the router login page without authentication.

How it works

The vulnerability starts with a poor authentication check for the router admin page, the attacker sends an arbitrary ping request to the device gateway interface that leads to command injection.Successful command injection allows attackers to gain complete control over the system, by gaining access to the device attackers can steal login credentials or install backdoor onto the server.

What to do

D-link said that “the products have entered End of Service Life. There is no support or development for these devices. We recommend replacing the device with a new device that is actively supported. Using these devices is at your own risk, D-Link does not recommend further use.”

Reference:

https://www.fortinet.com/blog/threat-research/d-link-routers-found-vulnerable-rce.html

Cisco Prime Infrastructure Health Monitor HA TarArchive - Directory Traversal / Remote Code Execution (*CVE-2019-1821, CVE-2019-1822 & CVE-2019-1823*) Severity: **HIGH**

Cisco has released patches for numerous vulnerabilities affecting its products, including Critical flaws in the Cisco Prime Infrastructure (PI) Software that could allow remote code execution.

How it works

The bugs impact the web-based management interface of Cisco PI and Cisco Evolved Programmable Network (EPN) Manager and could allow a remote attacker to execute arbitrary code with elevated privileges. Cisco explains in an advisory, CVE-2019-1821 can be exploited by an unauthenticated attacker with network access to the affected administrative interface.

CVE-2019-1822 and CVE-2019-1823, on the other hand, require that the attacker has valid credentials to authenticate to the impacted administrative interface.

What to do

These vulnerabilities are fixed in Cisco PI Software Releases 3.4.1, 3.5, and 3.6, and EPN Manager Release 3.0.1

Reference:

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190515-pi-rcel

Microsoft Windows Scripting Engine Memory Corruption Vulnerability *(CVE-2019-1429)*

Severity: **HIGH**

An information disclosure vulnerability exists when Microsoft Edge based on Edge HTML improperly handles objects in memory.

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.

What to do

Users of Microsoft are to apply appropriate patches or appropriate mitigations provided by Microsoft to vulnerable systems immediately

Reference

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1429

WordPress Unauthenticated View Posts Vulnerability (CVE- 2019-17671) Severity: **HIGH**

Wordpress versions allows unauthenticated view of private/draft posts. Unauthenticated viewing of certain content is possible because the static query property is mishandled.

How it works

This vulnerability could allow an unauthenticated user to view private or draft posts due to an issue within WP_Query

What to do

System Administrators and users, it is highly recommended to update WordPress to the latest version 5.2.4

Reference

https://wordpress.org/news/2019/10/wordpress-5-2-4-security-release/

Pulse Secure VPN Arbitrary Command Execution Vulnerability *(CVE- 2019-11539)* Severity: **HIGH**

Pulse Secure VPN with admin web interface allows an authenticated attacker to inject and execute commands.

How it works

An attacker can exploit these issues to access arbitrary files in the context of the application, write arbitrary files, hijack an arbitrary session and gain unauthorized access, execute arbitrary script code in the browser of an unsuspecting user in the context of the affected site, obtain sensitive information, inject and execute arbitrary commands and execute arbitrary code in the context of the application.

What to do

It is strongly recommended to update the corresponding version with the fix as soon as possible.

Reference

https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44101

Other Vulneabilities with known Exploits

rConfig Remote Code Execution Vulnerability (*CVE-2019-16662*) Severity: **HIGH**

Description: An issue was discovered in rConfig where an attacker can directly execute system commands by sending a GET request to ajaxServerSettingsChk.php because the rootUname parameter is passed to the exec function without filtering, which can lead to command execution

Kibana Timelion Remote Code Execution Vulnerability (*CVE-2019-7609*) Severity: **HIGH**

Description: Kibana Timelion visualizer is exposed to an arbitrary code execution vulnerability. An attacker with access to the Timelion application could send a request that will attempt to execute javascript code. This could possibly lead to an attacker executing arbitrary commands with permissions of the Kibana process on the host system.

Xorg X11 Server Local Privilege Escalation Vulnerability*(CVE-2018-14665)* Severity: **MEDIUM**

Description: A flaw was found in xorg-x11-server where an incorrect permission check for -modulepath and -logfile options are set when starting Xorg. X server allows unprivileged users with the ability to log in to the system via physical console to escalate their privileges and run arbitrary code under root privileges.

FusionPBX Operator Panel exec.php Command Execution Vulnerability *(CVE-2019-11409)* Severity: **HIGH**

Description: app/operator_panel/exec.php in the Operator Panel module in FusionPBX suffers from a command injection vulnerability due to a lack of input validation that allows authenticated non-administrative attackers to execute commands on the host. This can further lead to remote code execution when combined with an XSS vulnerability also present in the FusionPBX Operator Panel module.

Samsung Mobile Android Samsung TTS Privilege Escalation (*CVE-2019-16253*) Severity: **HIGH**

The Samsung Text-to-speech Engine System Component on Android suffers from a local privilege escalation vulnerability. The Text-to-speech Engine application for Android allows a local attacker to escalate privileges, e.g., to system privileges. A successful local attack can obtain system privilege on vulnerable phones.

GNU Mailutils Privilege Escalation Vulnerability *(CVE-2019-18862)* Severity: **HIGH**

Description: The --url parameter included in the GNU Mailutils maidag utility can be used to write to arbitrary files on the host operating system. By default, maidag is set to execute with setuid root permissions, which can lead to local privilege escalation through code/command execution by writing to the system's crontab or by writing to other root owned files on the operating system.

Other Vulnerabilities

- **Bludit Directory Traversal Image File Upload Vulnerability**

Bludit allows remote code execution via bl-kernel/ajax/upload-images.php because PHP code can be entered with a .jpg file name, and then this PHP code can write other PHP code to a ../ pathname.

- **Nostromo Nhttpd Remote Code Execution Vulnerability**

A Directory Traversal vulnerability exists in the function http_verify in nostromo nhttpd. It allows an attacker to achieve remote code execution via a crafted HTTP request. An attacker can bypass a check for /../ which allows to execute /bin/sh with arbitrary arguments.

Compiled with information from SANS' @RISK: The Concensus Security Vulnerability Alerts.

The Severity ratings on each vulnerabilities are shown with HIGH and MEDIUM were taken from NIST CVSS 2.0 version National Vulnerability Database (NVD).

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