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

TLP: White[1]

Security Bulletin – December 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

Apache Httpd mod_proxy Error Page Cross-Site Scripting Vulnerability(*CVE-2019-10092*)

Severity: **HIGH**

A limited cross-site scripting issue was reported affecting the mod_proxy error page.

How it works

An attacker could cause the link on the error page to be malformed and instead point to a page of their choice. This would only be exploitable where a server was set up with proxying enabled but was misconfigured in such a way that the Proxy Error page was displayed..

What to do

Apache has recommended updating to the latest version which have included fix for all vulnerabilities with the version of apache httpd 2.4.41

Reference:

http://httpd.apache.org/security/vulnerabilities_24.html

Android-Gif-Drawable Whatsapp Double Free 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/

Revive Adserver Remote Code Execution Vulnerability (*CVE-2019-5434*) Severity: **HIGH**

A vulnerability has been discovered in the Revive Adserver's delivery XML-RPC scripts. Such vulnerability could be used to perform various types of attacks, e.g. exploit serialize-related PHP vulnerabilities or PHP object injection.

How it works

An attacker could send a specifically crafted payload to the XML-RPC invocation script and trigger the unserialize() call using the "what" parameter in the "openads.spc" RPC method of adxmlrpc.php and www/delivery/axmlrpc.php. Likewise the www/delivery/dxmlrpc.php script uses unserialize() on the first parameter of the "pluginExecute" method.

What to do

It is strongly advise users to upgrade to the most recent 4.2.0 version of Revive Adserver as soon as possible.

Reference:

https://www.revive-adserver.com/security/revive-sa-2019-001/

Cisco Wireless LAN Controller Denial of Service Vulnerability (*CVE-2019-15276*) Severity: **HIGH**

A vulnerability in the web interface of Cisco Wireless LAN Controller Software could allow a low-privileged, authenticated, remote attacker to cause a denial of service (DoS) condition on an affected device.

How it works

An attacker could exploit this vulnerability by authenticating with low privileges to an affected controller and submitting the crafted URL to the web interface of the affected device. The unauthenticated attacker could exploit this vulnerability by persuading a user of the web interface to click the crafted URL. A successful exploit could allow the attacker to cause an unexpected restart of the device, resulting in a DoS condition.

What to do

Cisco has released software updates that may address this vulnerability. Please do update as soon as possible.

Reference:

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191106-wlc-dos

Trend Micro Deep Security Agent 11 Arbitrary File Overwrite Vulnerability (*CVE-2019-15627*) Severity: **HIGH**

Trend Micro Deep Security Agent are vulnerable to an arbitrary file delete attack, which may lead to availability impact.

How it works

The attack requires access to local operating system. The vulnerability allows an unprivileged local attacker to delete any file on the filesystem, or overwrite it with abritrary data hosted elsewhere.

What to do

Trend Micro has highly encouraged to update to the latest versions as soon as possible

Reference:

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

OpenBSD Dynamic Loader Privilege Escalation Vulnerability (*CVE-2019-19726*) Severity: **HIGH**

A local privilege escalation vulnerability exisys in OpenBSD's dynamic loader. This vulnerability is exploitable in the default installation (via the set-user-ID executable chpass or passwd) and could allow local users or malicious software to gain full root privileges.

How it works

OpenBSD through 6.6 allows local users to escalate to root because a check for LD_LIBRARY_PATH in setuid programs can be defeated by setting a very small RLIMIT_DATA resource limit. When executing chpass or passwd (which are setuid root), _dl_setup_env in ld.so tries to strip LD_LIBRARY_PATH from the environment, but fails when it cannot allocate memory. Thus, the attacker is able to execute their own library code as root.

What to do

OpenBSD has released software updates that may address this vulnerability. Please do update as soon as possible.

Reference:

https://www.openbsd.org/errata66.html

Mozilla Firefox Multiple Vulnerabilities *(CVE-2019-11708, CVE-2019-9810)* Severity: **HIGH**

This is a full browser compromise exploit chain targeting Mozilla Firefox on Windows 64-bit. It uses CVE-2019-9810 for getting code execution in both the content process as well as the parent process and CVE-2019-11708 to trick the parent process into browsing to an arbitrary URL. Insufficient vetting of parameters passed with the Prompt:Open IPC message between child and parent processes can result in the non-sandboxed parent process opening web content chosen by a compromised child process. When combined with additional vulnerabilities this could result in executing arbitrary code on the user's computer.

How it works

A remote attacker could entice a user to view a specially crafted web page, possibly resulting in the execution of arbitrary code with the privileges of the process or a Denial of Service condition.

What to do

Users of Mozilla firefox are highly urge to apply appropriate patches or appropriate mitigations provided by Mozilla.

Reference

https://www.mozilla.org/en-US/security/advisories/mfsa2019-19/

https://www.mozilla.org/en-US/security/advisories/mfsa2019-10/

Adobe Acrobat Reader Heap Based Memory Corruption Vulnerability *(CVE-2019-16451)* Severity: **HIGH**

Adobe Acrobat and Reader versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version,

2017.011.30152 and earlier, and 2015.006.30505 and earlier have a heap overflow corruption vulnerability exists in Adobe Acrobat Reader.

How it works

This vulnerability in Acrobat Reader for Windows, allows access violation exception when opening a malformed PDF file. Successful exploitation could lead to arbitrary code execution.

What to do

Adobe recommends users update their software installations to the latest versions

Reference

https://helpx.adobe.com/security/products/acrobat/apsb19-55.html

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

Lenovo Power Management Driver Denial of Service Vulnerability *(CVE-2019-6192)* Severity: HIGH

A potential vulnerability has been reported in the Lenovo Power Management Driver which could lead to a denial of service.

How it works

The vulnerability exists due to insuffiecient input buffer validation when the driver processes IOCTL codes Attackers can exploit this issue to cause a Denial of Service or possibly execute arbitrary code in kernel space.

What to do

Users are to update your Lenovo Power Management driver version 1.67.17.48 or higher

Reference

https://support.lenovo.com/us/en/solutions/len-29334

Other Vulneabilities with known Exploits

Integard Pro Remote Buffer Overflow Vulnerability (*CVE-2019-16702*) Severity: **HIGH**

Description: Integard Pro allows remote attackers to execute arbitrary code via a buffer overflow involving a long NoJs parameter to the /LoginAdmin URI. Integard fails to sanitize input to the "NoJs" parameter in an HTTP POST request# resulting in a stack buffer overflow that overwrites the instruction pointer, leading to remote code execution.

AppXSvc Arbitrary File Overwrite Denial of Service Vulnerability *(CVE-2019-16451)* Severity: **HIGH**

Description: An elevation of privilege vulnerability exists when the AppX Deployment Server (AppXSvc) improperly handles file hard links. AppXSvc can be forced to overwrite an arbitrary file by deleting all registry data files before creating the file hard link. A low privileged user could exploit this vulnerability to cause denial of service by overwriting critical system files.

.

Other Vulnerabilities

- **Verot Remote Code Execution Vulnerability** (*CVE-2019-19576*) Severity: **HIGH**

Description: Verot versions are exposed to remote code execution vulnerability. class.upload.php in verot.net class.upload, as used in the K2 extension for Joomla! and other products, omits .phar from the set of dangerous file extensions.

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