certTonga

Tonga National Computer Emergency Response Team

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

TLP: White[1]

Security Bulletin – September 2019

Dear Constituents,

As for the cyber security has increased, the threats and the risk on on High Alert. This is a security alert in advising our people in making sure that they stay alert on the cyber threats and how to mitigate such risks.

Vulnerabilities with Active Exploits in the Wild

Cisco Routers Remote Command Execution Vulnerability *(CVE-2019-1663)*- SEVERITY- ***High***

A vulnerability in the web-based management interface of the Cisco RV110W Wireless-N VPN Firewall, Cisco RV130W Wireless-N Multifunction VPN Router, and Cisco RV215W Wireless-N VPN Router.

How it works

This could allow an unauthenticated, remote attacker to execute arbitrary code on an affected device. The vulnerability is due to improper validation of user-supplied data in the web-based management interface. A remote attacker can exploit this issue to execute arbitrary commands on the host operating system with escalated privileges.

What to do

Cisco has released free software updates that address the vulnerability.

- Customers may only install and expect support for software versions and feature sets for which they have purchased a license. By installing, downloading, accessing, or otherwise using such software upgrades, customers agree to follow the terms of the Cisco software license

Updated version for Cisco products.

- RV110W Wireless-N VPN Firewall: 1.2.2.1
- RV130W Wireless-N Multifunction VPN Router: 1.0.3.45
- RV215W Wireless-N VPN Router: 1.3.1.1

[1] CERT Tonga adopts the Traffic Light Protocol

Reference

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190227-rmi-cmd-ex

WordPress Plugin Photo Gallery Cross-Site Scripting Vulnerability *(CVE-2019-16118)* SEVERITY- ***High***

Photo Gallery is an advanced Plugin with a list of tools and options for adding and editing images for different views. There are more than 100,000 installs worldwide. This plugin is exposed to a cross site scripting (XSS) vulnerability via admin/controllers/Options.php.

How it works

- This vulnerability occurs whenever an application includes untrusted data in a new web page without proper validation or escaping, or updates an existing web page with user supplied data using a browser API that can create JavaScript.
- The vulnerability allows attackers to execute scripts in the victim’s browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.

What to do

Administrators and Users of WordPress are advised to update Photo Gallery Plugin to the latest version 1.81

Reference

Wordpress- https://wordpress.org/plugins/simple-photo-gallery/#developers

Microsoft DirectWrite Information Disclosure Vulnerability *(CVE-2019-1245)*SEVERITY- ***Medium***

An information disclosure vulnerability exists when DirectWrite improperly discloses the contents of its memory.

How it works

An attacker who successfully exploited the vulnerability could obtain information to further compromise the user’s system.

There are multiple ways an attacker could exploit the vulnerability, such as by convincing a user to open a specially crafted document, or by convincing a user to visit an untrusted web-page.

What to do

Users who has microsoft products, can get regularly updates from website.

Reference

Microsoft-https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1093

New Zero Day Flaw affecting most Android Phones *(CVE-2019-2215)*

SEVERITY- ***High***

A critical unpatched zero-day vulnerability, this time in the world's most widely used mobile operating system, Android.

How it works

The zero-day is a use-after-free vulnerability in the Android kernel's binder driver that can allow a local privileged attacker or an app to escalate their privileges to gain root access to a vulnerable device and potentially take full remote control of the device.

Affected Android Device includes:

- Pixel 1
- Pixel 1 XL
- Pixel 2
- Pixel 2 XL
- Huawei P20
- Xiaomi Redmi 5A
- Xiaomi Redmi Note 5
- Xiaomi A1
- Oppo A3
- Moto Z3
- Oreo LG phones
- Samsung S7
- Samsung S8
- Samsung S9

What to do

As for Android users, it is highly recommended to update the firmware version of your android device to the latest.

Reference

Google Project Zero: https://bugs.chromium.org/p/project-zero/issues/detail?id=1942#c7

phpMyAdmin Cross Site Request Forgery Vulnerability *(CVE-2019-14654)*

SEVERITY- ***High***

A Cross site request forgery issue in phpMyAdmin allows deletion of any server in the Setup page.

How it works

The attacker can easily create a fake hyperlink containing the request that wants to execute on behalf the user,in this way making possible a CSRF attack due to the wrong use of HTTP method.

What to do

Upgrade to phpMyAdmin 4.9.0 or newer version

Reference

phpadmin- https://www.phpmyadmin.net/security/PMASA-2019-4/

Microsoft Windows AppXSvc Elevation of Privilege Vulnerability *(CVE-2019-1253)*

SEVERITY- ***High***

An elevation of privilege vulnerability exists when the Windows AppX Deployment Server improperly handles junctions

An information disclosure vulnerability exists when certain central processing units speculatively access memory. An attacker who successfully exploited the vulnerability could read privileged data across trust boundaries.

How it works

An attacker who successfully exploited this vulnerability could run processes in an elevated context. An attacker could then install programs; view, change or delete data. To exploit this vulnerability, an attacker would first have to log on to the system.

Also the attacker could then run a specially crafted application that could exploit the vulnerability and take control of an affected system.

What to do

Apply the most recent upgrade or patch from Microsoft website.

Reference

Microsoft - https://portal.msrc.microsoft.com/en-us/security-guidance

Exim Remote Command Execution Vulnerability *(CVE-2019-10149)*

SEVERITY- ***High***

A vulnerability has been discovered in Exim, which could allow for unauthenticated remote attackers to execute arbitrary system commands on the mail server.

How it works

A vulnerability has been discovered in Exim, which could allow for unauthenticated remote attackers to execute arbitrary system commands by sending a large specially crafted Extended HELO (EHLO) string to the mail server.

This vulnerability exists due to a heap buffer overflow vulnerability within the string_vformat() function in string.c. This function does not account for the size of the input string and can therefore lead to a buffer overflow condition. This can lead the mail server process to crash and potentially allow for remote code execution.

What to do

Please ensure to download and update to the latest version.

Reference

Exim: https://www.exim.org/static/doc/security/CVE-2019-10149.txt

Other Vulneabilities with known Exploits

Cisco UCS Director Unauthenticated Remote Access Vulnerability (CVE-2019-1935) SEVERITY- ***High***

A vulnerability in Cisco Integrated Management Controller (IMC) Supervisor, Cisco UCS Director, and Cisco UCS Director Express for Big Data could allow an unauthenticated, remote attacker to log in to the CLI of an affected system by using the SCP User account (scpuser), which has default user credentials. The vulnerability is due to the presence of a documented default account with an undocumented default password and incorrect permission settings for that account. Due to several coding errors, it is possible for an unauthenticated remote attacker with no privileges to bypass authentication and abuse a password change function to inject arbitrary commands and execute code
as root. An attacker could exploit this vulnerability by using the account to log in to an affected system. A successful exploit could allow the attacker to execute arbitrary commands with the privileges of the scpuser account.

LibreNMS Collectd Command Injection Vulnerability *(CVE-2019-15107)*

SEVERITY- ***High***

LibreNMS is exposed to a command injection vulnerability in html/includes/graphs/device/collectd.inc.php where user supplied parameters are filtered with the mysqli_escape_real_string function. This function is not the appropriate function to sanitize command arguments as it does not escape a number of command line syntax characters such as ` (backtick), allowing an attacker to inject commands into the variable $rrd_cmd, which gets executed via passthru(). An authenticated attacker can execute commands on the server.

Pulse Secure SSL VPN Remote Code Execution Vulnerability (*CVE-2019-11539)*

SEVERITY- ***High***

In Pulse Secure Pulse Connect Secure and Pulse Policy Secure, the admin web interface allows an authenticated attacker to inject and execute commands. 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.

Other Vulnerabilities

- **October CMS build 412 PHP code execution Vulnerability**

October CMS build 412 is vulnerable to PHP code execution vulnerability in the file upload functionality resulting in site compromise and possibly other applications on the server. The vunerability allows an attacker to execute PHP code on a victim's website where the attacker is an authenticated administrator user with media or asset management permissions.

- **FusionPBX Remote Code Execution Vulnerability**

FusionPBX allows an attacker to execute arbitrary system commands by submitting a malicious command to the service_edit.php file (which will insert the malicious command into the database). To trigger the command, one needs to call the services.php file via a GET request with the service id followed by the parameter a=start to execute the stored command.

- **DASAN Zhone ZNID GPON 2426A EU Device Multiple Cross-Site Scripting Vulnerabilities**

Multiple Cross-Site Scripting issues in the web interface on DASAN Zhone ZNID GPON 2426A EU devices allow a remote attacker to execute arbitrary JavaScript via manipulation of an unsanitized GET parameter: /zhndnsdisplay.cmd (name), /wlsecrefresh.wl (wlWscCfgMethod, wl_wsc_reg).

- **Symantec Advanced Secure Gateway Unrestricted File Upload Vulnerability**

An Unrestricted file upload vulnerability exists in the Symantec Advanced Secure Gateway (ASG) and ProxySG management consoles. A malicious appliance administrator can upload arbitrary malicious files to the management console and trick another administrator user into downloading and executing malicious code.

- **Western Digital My Book World II NAS Authentication Bypass Vulnerability**

An Authentication Bypass Vulnerability exists in Western Digital WD My Book World, which allows an attacker to access the /admin/ directory without credentials. An attacker can easily enable SSH from /admin/system_advanced.php?

- **Tableau XML External Entity Injection Vulnerability**

Numerous Tableau products are vulnerable to XXE (XML External Entity) vulnerability beacuse of a malicious workbook, extension, or data source, leading to information disclosure or a denial of service vulnerability. This affects Tableau Server, Tableau Desktop, Tableau Reader, and Tableau Public Desktop.

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

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

Disclaimer Notice:
The information in this notice is intended solely for public knowledge and awareness, and not intending to harm, fright or disturb any person(s), legal entity or the receiver of this information. Under no circumstances shall the Ministry of MEIDECC be liable for any indirect, incidental, consequential, special or exemplary damages arising out of or in connection with your access or use of or inability to access or use the information and any third party content and services