Tonga National Computer Emergency Response Team

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

TLP: White[1]

Security Bulletin – October 2019

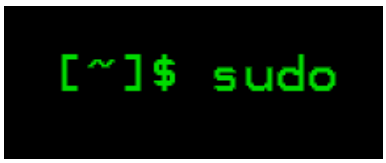
Dear Constituents,

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

Sudo Security Bypass Vulnerability (CVE-2019-11932)- Severity: High

A new vulnerability has been discovered in **Sudo**—one of the most important, powerful, and commonly used utilities that comes as a core command installed on almost every UNIX and Linux-based operating system.



How it works

When sudo is configured to allow a user to run commands as an arbitrary user via the ALL keyword in a Run as specification. It is possible to run commands as root by specifying the user ID -1 or 4294967295. This can be used by a user with sufficient sudo privileges to run commands as root even if the Runas specification explicitly disallows root access as long as the ALL keyword is listed first in the Runas specification. 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.

What to do

The vulnerability affects all Sudo versions prior to the latest released version 1.8.28, which has been released.

Reference

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

1 CERT Tonga adopts the Traffic Light Protocol

D-Link Unauthenticated Command-Injection Vulnerability (CVE-2019-16920)- Severity: **High**

The vulnerability exists in the latest firmware for the DIR-655, DIR-866L, DIR-652 and DHP-1565 products, which are Wi-Fi routers.

How it works

The vulnerability exists due to improper sanitization of arbitrary commands that are executed by the native command-execution function. An attacker who successfully triggers the command injection could achieve full system compromise.

What to do

Users to get the latest update firmware of D-Link router. Please refer to Reference for more information

Reference

D-Link:https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10124

TP-Link Authentication Bypass Vulnerability (CVE-2019-6971)- Severity: **High**

An issue was discovered on TP-Link TL-WR1043ND V2 devices.

How it works

An attacker can send a cookie in an HTTP authentication packet to the router management web interface, and fully control the router without knowledge of the credentials.

What to do

For users and system administrators to update your TP link firmware to the latest updates

Reference

https://github.com/MalFuzzer/Vulnerability-Research/blob/master/TL-WR1043ND%20V2%20-%20TP-LINK/TL-WR1043ND_PoC.pdf

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

A double free vulnerability in the DDGifSlurp function in decoding.c in libpl_droidsonroids_gif, as used in WhatsApp for Android, leading to Denial of Services

How it works

Exploiting the vulnerability can allow a malicious actor to escalate privileges on a compromised Android phone and gain access to files stored on the device, including the WhatsApp messages database. It can also be used to create a remote shell in the context of

WhatsApp.Exploitation involves sending a malicious GIF file, which automatically triggers the vulnerability when the targeted user opens the WhatsApp Gallery; for example, when they want to send a picture to one of their contacts.

What to do

It is recommended that WhatsApp users accept automatic updates to their software to stay protected.

Reference

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

Exim Remote Command Execution Vulnerability (CVE-2019-16928) 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

Download and Update to the fixed version 4.92

Reference

Exim: https://www.exim.org/static/doc/security/CVE-2019-16928.txt

Cisco Small Business 220 Series Smart Switches Vulnerabilities (CVE-2019-1912), (CVE-2019-1913) Severity: **High** & (CVE-2019-1914) Severity: **Medium**

Cisco has patched three dangerous bugs in one of its most popular products, the Cisco Small Business 220 Series of smart switches.

How it works

Of the three, the first two are the most dangerous because they can be exploited by remote attackers over the internet without needing to authenticate on the device. This means that any Cisco 220 Series smart switch that is reachable over the internet can be attacked.

What to do

The three vulnerabilities reside in the switches' web management interface. Owners can either turn off the web management interface or install the updates Cisco released.

The fix is incorporated in the firmware version 1.1.4.4 or later. All previous versions are to be considered vulnerable.

References

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190806-sb220-auth_bypass
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190806-sb220-rce
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190806-sb220-inject

Microsoft Internet Explorer Remote Code Execution Vulnerability (CVE-2019-1367)

Severity: **High**

A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user.

How it works

An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Internet Explorer and then convince a user to view the website, for example, by sending an email

What to do

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

Reference

Microsoft: https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1367

Other Vulneabilities with known Exploits

Android Binder Use-After-Free Vulnerability (CVE-2019-2215) Severity- **Medium**

A use after free in binder.c allows an elevation of privilege from an application to the Linux Kernel. No user interaction is required to exploit this vulnerability, however exploitation does require either the installation of a malicious local application or a separate vulnerability in a network facing application.

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

Kibana Timelion visualizer is exposed to an arbitrary code execution vlunerability. An attacker with acces 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.

vBulletin pre-authentication remote code execution vulnerability (CVE-2019-16759*)* Severity- **High**

An unauthenticated attacker can send a specially crafted HTTP POST request to a vulnerable vBulletin host and execute commands. These commands would be executed with the permissions of the user account

that the vBulletin service is utilizing.The vulnerability would enable an attacker to hijack the webserver running the forum software, to launch attacks on other machines and to modify and steal sensitive information.

DotNetNuke Store Cross-Site Scripting vulnerability (CVE-2019-12562)

Severity- **Medium**

A stored cross site scripting vulenrability in DotNetNuke (DNN) allows remote attackers to store and embed the malicious script into the admin notification page. The exploit could be used to perfom any action with admin privileges such as managing content, adding users, uploading backdoors to the server, etc. Successful exploitation occurs when an admin user visits a notification page with stored cross-site scripting.

Anchor CMS Information Disclosure Vulnerability (CVE-2019-11932) Severity- **High**

A double free vulnerability in the DDGifSlurp function in decoding.c in libpl_droidsonroids_gif as used in WhatsApp for Android, allows remote attackers to execute arbitrary code or cause a denial of service. By default, AnchorCMS will log errors to the "/anchor/errors.log" file in the webroot of the web application. This allows malicious users to access the error log and view potentially sensitive information.

Microsoft Scripting Engine Memory Corruption Vulnerability (CVE-2019-1367) Severity- **High**

A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer. 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.

Pulse Connect Secure arbitrary file read vulnerability (CVE-2019-11510) Severity- **High**

In Pulse Secure Pulse Connect Secure (PCS) 8.2 before 8.2R12.1, 8.3 before 8.3R7.1, and 9.0 before 9.0R3.4, an unauthenticated remote attacker can send a specially crafted URI to perform an arbitrary file reading vulnerability .

Other Vulnerabilities

- **Kirona-DRS Information Disclosure Vulnerability**

An information disclosure vulnerability exists in Kirona Dynamic Resource Scheduling (DRS). An unauthenticated user can access /osm/REGISTER.cmd (aka /osm_tiles/REGISTER.cmd) directly that contains sensitive information about the database through the SQL queries within this batch file. This file exposes SQL database information such as database version, table name, column name, etc

- **Harbor Remote Privilege Escalation Vulnerability**

A vulnerability in the POST /api/users API of Harbor may allow for a remote escalation of privilege. A malicious attacker with network access to a Harbor POST /api/users API could self-register a new account

with administrative privileges. Successful exploitation of this issue may lead to a complete compromise of the Harbor deployment.

- **Counter-Strike Global Offensive Remote Code Execution Vulnerability**

Counter-Strike Global Offensive (vphysics.dll) allows remote attackers to achieve code execution or denial of service by creating a gaming server and inviting a victim to this server, using a crafted map that causes memory corruption vulnerability.

- **IBM Bigfix Platform Arbitrary File Upload Vulnerability**

IBM BigFix Platform could allow any authenticated user to upload any file to any location on the server with root privileges. This results in code execution on underlying system with root privileges. An attacker can for example upload script file on the web server and execute it by sending GET request

- **Cisco Small Business 220 Series Smart Switches Command Injection Vulnerability**

A vulnerability in the web management interface of Cisco Small Business 220 Series Smart Switches could allow an authenticated, remote attacker to perform a command injection attack. The vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending a malicious request to certain parts of the web management interface. To send the malicious request, the attacker needs a valid login session in the web management interface as a privilege level 15 user. Depending on the configuration of the affected switch, the malicious request must be sent via HTTP or HTTPS. A successful exploit could allow the attacker to execute arbitrary shell commands with the privileges of the root user.

- **ThinVNC Authentication Bypass Vulnerability**

ThinVNC 1.0b1 is vulnerable to arbitrary file read, which leads to a compromise of the VNC server. The vulnerability exists even when authentication is turned on during the deployment of the VNC server. The password for authentication is stored in cleartext in a file that can be read via a ../../ThinVnc.ini directory traversal attack vector.

- **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

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