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

TLP: White[1]

Security Bulletin – January 2020

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

FreeBSD Privilege Escalation Vulnerability (*CVE-2019-5596*) Severity: HIGH

A bug in the reference count implementation for UNIX domain sockets can cause a file structure to be incorrectly released potentially allowing a malicious local user to gain root privileges or escape from a jail

How it works

The code which performs this operation failed to release a reference obtained on the file corresponding to a received right. This bug can be used to cause the reference counter to wrap around and free the file structure.
A local attacker can exploit this issue to gain root privileges or cause denial-of-service condition.

What to do

Free BSD has recommended updating to the latest version which have included fix for all vulnerabilities with the stable version of freeBSD 12.0 or 12.1.

Reference

https://www.freebsd.org/security/advisories/FreeBSD-SA-19:02.fd.asc

Citrix ADC & Citrix Gateway Arbitrary Code Execution Vulnerability(*CVE- 2019-19781)* Severity: HIGH

A vulnerability has been identified in Citrix Application Delivery Controller (ADC) formerly known as NetScaler ADC and Citrix Gateway formerly known as NetScaler Gateway.

1 CERT Tonga adopts the Traffic Light Protocol

How it works

It could allow an unauthenticated attacker to perform arbitrary code execution, this vulnerability includes Citrix ADC and Citrix Gateway Virtual Appliances (VPX) hosted on any of Citrix Hypervisor (formerly XenServer), ESX, Hyper-V, KVM, Azure, AWS, GCP or on a Citrix ADC Service Delivery Appliance (SDX)

What to do

Citrix has recommended and have release patches for the affected appliances, so please update as soon as possible.

Reference

https://support.citrix.com/article/CTX267027

Microsoft UPnP Local Privilege Elevation Vulnerability (*CVE-2019-1405*) Severity: **HIGH**

An elevation of privilege vulnerability exists when the Windows Universal Plug and Play (UPnP) service improperly allows COM object creation.

How it works

An attacker who successfully exploited this vulnerability could run arbitrary code with elevated system privileges. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted script or application.

What to do

It is strongly advise users to upgrade to the most recent versions as well as applying security patches from Microsoft.

Reference

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1405

Windows Shell COM Server Registrar Local Privilege Escalation Vulnerability (*CVE-2019-1184*) Severity: **HIGH**

An elevation of privilege vulnerability exists when Windows Core Shell COM Server Registrar improperly handles COM calls.

How it works

To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and take control of an affected system.

What to do

It is highly encouraged to have your (Windows) computer set to update automatically and also apply patch as soon as possible.

Reference:

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1184

Microsoft Windows CryptoAPI Spoofing Vulnerability (*CVE-2020-0601*) Severity: **MEDIUM**

A spoofing vulnerability exists in the way Windows CryptoAPI (Crypt32.dll) validates Elliptic Curve Cryptography (ECC) certificates.

How it works

An attacker could exploit the vulnerability by using a spoofed code-signing certificate to sign a malicious executable, making it appear the file was from a trusted, legitimate source. The user would have no way of knowing the file was malicious, because the digital signature would appear to be from a trusted provider.

What to do

It is strongly advice to apply Microsoft patches as soon as possible

Reference:

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0601

Microsoft Windows Search Indexer Elevation of Privilege Vulnerability *(CVE-2020-0632)*

Severity: **MEDIUM**

An elevation of privilege vulnerability exists in the way that the Windows Search Indexer handles objects in memory.

How it works

An attacker who successfully exploited the vulnerability could execute code with elevated permissions. To exploit the vulnerability, a locally authenticated attacker could run a specially crafted application.

What to do

It is highly recommended to apply the most appropriate patch and update as soon as possible

Reference

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0632

VMWare Privilege Escalation Vulnerability *(CVE-2020-3941)* Severity: **MEDIUM**

A vulnerability exists in VMware Tools for windows, which may allow for privilege escalation in the Virtual Machine where Tools is installed.

How it works

A malicious actor on the guest VM might exploit the race condition and escalate their privileges on a Windows VM.

What to do

It is highly recommended to update VMware Tools version to 11.0 or later

Reference

https://www.vmware.com/security/advisories/VMSA-2020-0002.html

OpenSSL Vulnerability (*CVE-2019-1547*) Severity: **LOW**

The OpenSSL EC groups always have a co-factor present and this is used in side channel resistant code paths. However, in some cases, it is possible to construct a group using explicit parameters (instead of using a named curve). In those cases it is possible that such a group does not have the cofactor present. This can occur even where all the parameters match a known named curve.

If such a curve is used then OpenSSL falls back to non-side channel resistant code paths which may result in full key recovery during an ECDSA signature operation.

How it works

In order to be vulnerable an attacker would have to have the ability to time the creation of a large number of signatures where explicit parameters with no co-factor present are in use by an application using libcrypto.

What to do

It is strongly advise users to upgrade to the most recent versions as soon as possible:

- OpenSSL 1.1.1 users should upgrade to 1.1.1d
- OpenSSL 1.1.0 users should upgrade to 1.1.0l
- OpenSSL 1.0.2 users should upgrade to 1.0.2t

Reference:

https://www.openssl.org/news/secadv/20190910.txt

Other Vulneabilities with known Exploits

Synaptics Audio Driver Vulnerability *(CVE-2019-9730)* Severity: **HIGH**

Description: Incorrect access control in the CxUtilSvc.exe component of the Synaptics (previously Conexant) Audio driver could allow a standard user to increase access privileges to the Windows Registry via an unpublished API.

Nostromo Web Server Unauthenticated Remote Code Execution Vulnerability (*CVE-2019-16278*) Severity: **HIGH**

Description: A remote code execution vulnerability exists in Nostromo Web Server. This issue is caused by a directory traversal in the function http_verify in nostromo nhttpd allowing an attacker to achieve remote

code execution via a crafted HTTP request. After successful exploitation of this vulnerability an attacker can achieve remote code execution via a crafted HTTP request.

OSIsoft Cross Site Request Forgery Vulnerability *(CVE-2019-18271)* Severity: **MEDIUM**

Description: The vulnerability exists due to insufficient validation of the HTTP request origin on the PI Vision administration site. A remote attacker can trick the victim to visit a specially crafted web page and perform arbitrary actions on behalf of the victim on the vulnerable website. The vulnerability allows a remote attacker to perform cross-site request forgery attacks.

OSIsoft Sensitive Information Disclosure Vulnerability *(CVE-2019-18244)* Severity: **LOW**

Description: The vulnerability exists due to the affected software records the service account password in the installation log files when a non-default service account and password are specified during installation or upgrade. A local attacker can gain access to sensitive information on the target system.

.

Other Vulnerabilities

Django count Hijack Vulnerability (*CVE-2019-19844*) Severity: **MEDIUM**

Description: Django allows account takeover. A suitably crafted email address (that is equal to an existing user's email address after case transformation of Unicode characters) would allow an attacker to be sent a password reset token for the matched user account. Django's password-reset form uses a case-insensitive query to retrieve accounts matching the email address requesting the password reset.

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

The Severity ratings on the above vulnerabilities are based on the NIST Common Vulnerability Scoring System Calculator (CVSS).

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