TLP: White[1]

Security Bulletin – December 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

VMware Workspace One Access Command Injection Vulnerability *(CVE-2020-4006)*

Severity: **HIGH**

Description

VMware Workspace One Access is exposed to a command injection vulnerability in the administrative configurator.

How it works

This could allow a malicious actor with network access to the administrative configurator on port 8443 and a valid password for the configurator admin account to execute commands with unrestricted privileges on the underlying operating system

What to do

Be sure to appropriate security updates recommended by vendor

Reference

https://www.vmware.com/security/advisories/VMSA-2020-0027.html

MobileIron Core and Connector Remote Code Execution Vulnerability *(CVE-2020-15505)*

Severity: **HIGH**

Description

A remote code execution vulnerability exists in MobileIron Core and Connector, and Sentry.

How it works

This allows remote attackers to execute arbitrary code via unspecified vectors. The manipulation with an unknown input leads to a privilege escalation vulnerability. The UK's National Cyber Security Centre alerts that APT nation-state groups and cybercriminals are exploiting MobileIron RCE vulnerability to compromise the networks.

1 CERT Tonga adopts the Traffic Light Protocol

What to do

Apply the appropriate security updates recommended

Reference

https://www.mobileiron.com/en/blog/mobileiron-security-updates-available

Apache Struts OGNL Remote Code Execution Vulnerability *(CVE-2020-17530)* Severity: HIGH

Description

A vulnerability found on Apache Struts OGNL

How it works

A vulnerability exists in the “forced OGNL evaluation on raw user input in tag attributes" of Apache Struts. Due to insufficient validation of user input in OGNL evaluation functionality, an unauthenticated user can exploit this flaw leading it to remote code execution vulnerability.

What to do

Ensure that you apply the most appropriate updates recommended by Vendor

Reference

https://cwiki.apache.org/confluence/display/WW/S2-061

Microsoft Kerberos Security Feature Bypass Vulnerability *(CVE-2020-17049)* Severity: HIGH

Description

A security feature bypass vulnerability exists in the way Key Distribution Center (KDC) determines if a service ticket can be used for delegation via Kerberos Constrained Delegation (KCD)

How it works

To exploit the vulnerability, a compromised service that is configured to use KCD could tamper with a service ticket that is not valid for delegation to force the KDC to accept it.

What to do

Make sure to apply appropriate security updates recommended by Microsoft.

Reference

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17049

F5 BIG-IP Remote Code Execution Vulnerability *(CVE-2020-5902)* Severity: **HIGH**

Description

F5 BIG-IP is exposed to remote code execution vulnerability.

How it works

The vulnerability that has been actively exploited in the wild allows attackers to read files, execute code or take complete control over vulnerable systems having network access.

What to do

Ensure to apply appropriate security updates recommended by vendor

Reference

https://support.f5.com/csp/article/K52145254

MacOS Catalina Memory Corruption Vulnerability *(CVE-2020-9844)* Severity: **HIGH**

Description

A double free issue was addressed with improved memory management

How it works

. A remote attacker may be able to cause unexpected system termination or corrupt kernel memory.

What to do

Apply the most appropriate security updates recommended by Apple.

Reference

https://support.apple.com/HT211170

https://support.apple.com/HT211168

Other Vulnerabilities with known Exploits

Microsoft Exchange Information Disclosure Vulnerability (*CVE-2020-17143)* Severity: **MEDIUM**

Description: Microsoft Exchange Server is exposed to information disclosure vulnerability that could be disclosed if an attacker successfully exploited this vulnerability for sensitive information.

Microsoft Windows SMB Information Disclosure Vulnerability (*CVE-2020-17140)* Severity: **MEDIUM**

Description: Microsoft Windows is exposed to SMB information disclosure vulnerability where an attacker can successfully exploit this vulnerability to access contents of Kernel memory. An attacker could read the contents of Kernel memory from a user mode process. In a network-based attack, an authenticated attacker would need to open a specific file with captured oplock lease, then perform repeated specific modifications to that file.

XStream Server-Side Forgery Request Vulnerability (*CVE-2020-26258)* Severity: **MEDIUM**

Description: A Server-Side Forgery Request vulnerability exists in XStream that can be activated when unmarshalling. The vulnerability may allow a remote attacker to request data from internal resources that are not publicly available only by manipulating the processed input stream

Adobe Experience Manager Server-Side Request Forgery Vulnerability (*CVE-2018-12809)* Severity: **MEDIUM**

Description: Adobe Experience Manager is exposed to server-side request forgery vulnerability. Successful exploitation could lead to sensitive information disclosure.

Google Android Play Core Library Arbitrary Code Execution Vulnerability (*CVE-2020-8913)* Severity: **MEDIUM**

Description: A local, arbitrary code execution vulnerability exists in the SplitCompat.install endpoint in Android's Play Core Library. A malicious attacker could create an app which targets a specific application, and if a victim were to install this app, the attacker could perform a directory traversal, execute code as the targeted application and access the targeted application's data on the Android device.

OpenSSL EDIPARTYNAME NULL pointer de-reference Vulnerability *(CVE-2020-1971*) Severity: **MEDIUM**

Description: A null pointer dereference flaw was found in openssl. A remote attacker, able to control the arguments of the GENERAL_NAME_cmp function, could cause the application, compiled with openssl to crash resulting in a denial of service. The highest threat from this vulnerability is to system availability.

Fortinet FortiOS Directory Traversal Vulnerability *(CVE-2018-13379*) Severity: **MEDIUM**

Description: Fortinet FortiOS is exposed to a directory traversal vulnerability because it fails to properly sanitize user supplied input. A path traversal vulnerability in the FortiOS SSL VPN web portal may allow an unauthenticated attacker to download FortiOS system files through specially crafted HTTP resource requests.

IBM Maximo Asset Management External Entity Injection Vulnerability (*CVE-2020-4463)* Severity: **MEDIUM**

Description: IBM Maximo Asset Management is vulnerable to an XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources.

containerd Privilege Escalation Vulnerability *(CVE-2020-15257*) Severity: **MEDIUM**

Description: The containerd-shim API is improperly exposed to host network containers. Access controls for the shim’s API socket verified that the connecting process had an effective UID of 0, but did not otherwise restrict access to the abstract Unix domain socket. This would allow malicious containers running in the same network namespace as the shim, with an effective UID of 0 but otherwise reduced privileges, to cause new processes to be run with elevated privileges.

Other Vulnerabilities

Kata Containers Improper File Permissions Vulnerability *(CVE-2020-28914)* Severity: **LOW**

Description: An improper file permissions vulnerability affects Kata Containers. When using a Kubernetes hostPath volume and mounting either a file or directory into a container as readonly, the file/directory is mounted as readOnly inside the container, but is still writable inside the guest. For a container breakout situation, a malicious guest can potentially modify or delete files/directories expected to be read-only.

Kubernetes Man In The Middle Vulnerability *(CVE-2020-8554)* Severity: **N/A**

Description: A man in the middle vulnerability exists in Kubernetes. The vulnerability could be exploited by users with very less privileges like creating services or editing services and pods in a Kubernetes cluster.

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) version 2.0

For more information please contact us:

CERT Tonga
Ministry of MEIDECC
Nuku'alofa
Tel: 2378 (CERT)
email: cert@cert.gov.to
web: www.cert.gov.to
Twitter: @CERTTonga | Facebook: @CERTTonga