TLP: White[1]

Security Bulletin – October 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

Oracle Weblogic Remote Code Execution Vulnerability *(CVE-2020-14882)* Severity: HIGH

Description

A critical vulnerability exists in Oracle WebLogic Server product of Oracle Fusion Middleware (component: Console).

How it works

Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server.

What to do

Apply the appropriate security updates recommended by Oracle

Reference

https://www.oracle.com/security-alerts/cpuoct2020.html

Adobe Flash Player Arbitrary Code Execution Vulnerability *(CVE-2020-9746)* Severity: HIGH

Description

A vulnerability exists in the Adobe Flash Player.

How it works

Adobe Flash Player is affected by an exploitable NULL pointer dereference vulnerability that could result in a crash and arbitrary code execution. Exploitation of this issue requires an attacker to insert malicious strings in an HTTP response that is by default delivered over TLS/SSL.

What to do

Be sure to appropriate security updates recommended by vendor

Reference

1 CERT Tonga adopts the Traffic Light Protocol

https://helpx.adobe.com/security/products/flash-player/apsb20-58.html

Cisco IOS XR Software Cisco Discovery Protocol Format String Vulnerability *(CVE-2020-3118)* Severity: **HIGH**

Description

A vulnerability in the Cisco Discovery Protocol implementation for Cisco IOS XR Software.

How it works

It could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability is due to improper validation of string input from certain fields in Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device.

What to do

Cisco has release the software updates that address the vulnerability, with no work around

Reference

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20200205-iosxr-cdp-rce

Cisco IOS XR Software DVMRP Memory Exhaustion Vulnerabilities *(CVE-2020-3566)*

Severity: **HIGH**

Description

A vulnerability in the Distance Vector Multicast Routing Protocol (DVMRP) feature of Cisco IOS XR Software

How it works

It could allow an unauthenticated, remote attacker to exhaust process memory of an affected device. The vulnerability is due to insufficient queue management for Internet Group Management Protocol (IGMP) packets. An attacker could exploit this vulnerability by sending crafted IGMP traffic to an affected device. A successful exploit could allow the attacker to cause memory exhaustion, resulting in instability of other processes.

What to do

Cisco has release the software updates that address the vulnerability.

Reference

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-dvmrp-memexh-dSmpdvfz

HP Device Manager Elevation of Privilege Vulnerability *(CVE-2020-6927)* Severity: **HIGH**

Description

A vulnerability found on HP Device Manager. The vulnerability is due to insufficient queue management for Internet Group Management Protocol (IGMP) packets.

How it works

These vulnerabilities may allow locally managed accounts within HP Device Manager to be susceptible to dictionary attacks due to weak cipher implementation and allow a malicious actor to remotely gain unauthorized access to resources, and/or allow a malicious actor to gain SYSTEM privileges

What to do

Ensure that you apply the most appropriate updates recommended by Vendor

Reference

https://support.hp.com/ca-en/document/c06921908

IBM QRadar Remote Java Script Deserialization Vulnerability *(CVE-2020-4280)* Severity: **HIGH**

Description

A Java deserialization vulnerability exists in the IBM QRadar Remote Java Script Servlet.

How it works

An authenticated user can call one of the vulnerable methods and cause the Servlet to deserialize arbitrary objects. An attacker can exploit this vulnerability by creating a specially crafted (serialized) object, which amongst other things can result in a denial of service, change of system settings, or execution of arbitrary code.

What to do

Apply the most appropriate security updates recommended by vendor

Reference

https://www.ibm.com/support/pages/node/6344079

Apache Solr ConfigSet Remote Code Execution Vulnerability *(CVE-2020-13957)* Severity: HIGH

Description

A vulnerability found in Apache Solr ConfigSet

How it works

Apache Solr allows some features to be configured in ConfigSet that's uploaded via API without authentication/authorization, which could be used for remote code execution. The checks in place to prevent such features can be circumvented by using a combination of UPLOAD/CREATE actions.

What to do

- Disable UPLOAD command in ConfigSets API if not used by setting the system property: "configset.upload.enabled" to "false"
- Use Authentication/Authorization and make sure unknown requests aren't allowed.
- Upgrade to Solr 8.6.3 or greater.
- If upgrading is not an option, consider applying the patch in SOLR-14663

Reference

https://mail-archives.us.apache.org/mod_mbox/www-announce/202010.mbox/%3CCAECwjAWCVLoVaZy%3DTNRQ6Wk9KWVxdPRiGS8NT%2BPHMJCxbbsEVg%40mail.gmail.com%3E

Microsoft Exchange Validation Key Remote Code Execution Vulnerability *(CVE-2020-0688)*

Severity: HIGH

Description

A remote code execution vulnerability exists in Microsoft Exchange Server when the server fails to properly create unique keys at install time.

How it works

Knowledge of a the validation key allows an authenticated user with a mailbox to pass arbitrary objects to be deserialized by the web application, which runs as SYSTEM.

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-2020-0688

Microsoft Windows Group Policy Elevation of Privilege Vulnerability *(CVE-2020-1013)*

Severity: HIGH

Description

An elevation of privilege vulnerability exists when Microsoft Windows processes group policy updates.

How it works

An attacker who successfully exploited this vulnerability could potentially escalate permissions or perform additional privileged actions on the target machine. To exploit this vulnerability, an attacker would need to launch a man-in-the-middle (MiTM) attack against the traffic passing between a domain controller and the target machine. An attacker could then create a group policy to grant administrator rights to a standard user.

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-2020-1013

Microsoft Windows Kernel Elevation of Privilege Vulnerability *(CVE-2019-1151)* Severity:

HIGH

Description

A remote code execution vulnerability exists when the Windows font library.

How it works

An attacker who successfully exploited the vulnerability could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

What to do

Ensure to apply appropriate security updates recommended by Microsoft.

Reference

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1151

Microsoft Exchange Server Remote Code Execution Vulnerability *(CVE-2020-1350)* Severity:

HIGH

Description

A remote code execution vulnerability exists in Windows Domain Name System servers when they fail to properly handle requests

How it works

An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the Local System Account. Windows servers that are configured as DNS servers are at risk from this vulnerability.

What to do

Ensure to apply appropriate security updates recommended by Microsoft.

Reference

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1350

Microsoft Windows Kernel Elevation of Privilege Vulnerability *(CVE-2020-1034)* Severity: **HIGH**

Description

An elevation of privilege vulnerability exists in the way that the Windows Kernel 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

Apply the most appropriate security updates recommended by Microsoft.

Reference

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1034

Other Vulnerabilities with known Exploits

Atlassian Jira Server and Data Center User Enumeration Vulnerability *(CVE-2020-14181)* Severity: **MEDIUM**

Description: Atlassian Jira Server and Data Center allow an unauthenticated user to enumerate users via an Information Disclosure vulnerability in the /ViewUserHover.jspa endpoint.

Microsoft SharePoint Remote Code Execution Vulnerability *(CVE-2020-16951)* Severity: **MEDIUM**

Description: A remote code execution vulnerability exists in Microsoft SharePoint when the software fails to check the source markup of an application package. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the SharePoint application pool and the SharePoint server farm account. Exploitation of this vulnerability requires that a user uploads a specially crafted SharePoint application package to an affected version of SharePoint.

Microsoft SQL Server Remote Code Execution Vulnerability *(CVE-2020-0618)* Severity: **MEDIUM**

Description: A remote code execution vulnerability exists in Microsoft SQL Server Reporting Services when it incorrectly handles page requests. An attacker who successfully exploited this vulnerability could execute code in the context of the Report Server service account.

To exploit the vulnerability, an authenticated attacker would need to submit a specially crafted page request to an affected Reporting Services instance.

Pulse Connect Secure Arbitrary Code Execution Vulnerability *(CVE-2020-8243*) Severity: **MEDIUM**

Description: A vulnerability exists in the Pulse Connect Secure admin web interface that could allow an authenticated attacker to upload custom template to perform an arbitrary code execution.

Mozilla Firefox User-After-Free Vulnerability *(CVE-2020-15675*) Severity: **MEDIUM**

Description: A user-after-free vulnerability exists in WebCGL in Mozilla Firefox. When processing surfaces, the lifetime may outlive a persistent buffer leading to memory corruption and a potentially exploitable crash.

Microsoft Windows Kernel Information Disclosure Vulnerability *(CVE-2020-16938*) Severity: **MEDIUM**

Description: An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory. An attacker who successfully exploited this vulnerability could obtain information to further compromise the user's system. To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application. The vulnerability would not allow an attacker to execute code or to elevate user rights directly, but it could be used to obtain information that could be used to try to further compromise the affected system.

Microsoft Windows TCP/IP Stack Remote Code Execution Vulnerability *(CVE-2020-16898*) Severity: **MEDIUM**

Description: A remote code execution vulnerability exists when the Windows TCP/IP stack improperly handles ICMPv6 Router Advertisement packets. An attacker who successfully exploited this vulnerability could gain the ability to execute code on the target server or client. To exploit this vulnerability, an attacker would have to send specially crafted ICMPv6 Router Advertisement packets to a remote Windows computer.

Apache Tomcat Unexpected Resource Response Vulnerability *(CVE-2020-13943*) Severity: **MEDIUM**

Description: If an HTTP/2 client exceeded the agreed maximum number of concurrent streams for a connection (in violation of the HTTP/2 protocol), it was possible that a subsequent request made on that connection could contain HTTP headers - including HTTP/2 pseudo headers - from a previous request rather than the intended headers. This could lead to users seeing responses for unexpected resources.

Instagram App Heap Buffer Overflow Vulnerability (*CVE-2020-1895)* Severity: **MEDIUM**
Description:A large heap overflow could occur in Instagram for Android when attempting to upload an image with specially crafted dimensions.

Google Chrome on Android Insufficient Bounds Check Vulnerability *(CVE-2020-6506)*

Severity: **MEDIUM**

Description: Insufficient policy enforcement in WebView in Google Chrome on Android allows a remote attacker to bypass site isolation via a crafted HTML page. An Android WebView instance with default configuration and JavaScript enabled allows an iframe on a different origin to bypass same-origin policies and execute arbitrary JavaScript in the top document.

Other Vulnerabilities

Gitea Authenticated Remote Code Execution Vulnerability *(CVE-2020-14144*) Severity: **MEDIUM**

Description: A vulnerability exists in Gitea, that allows an attacker with access to an administrative account or an account with special privileges to execute arbitrary code on the server.

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