TLP: White[1]

Security Bulletin – February 2021

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

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

Description

Apache Solr versions 6.6.0 to 6.6.6, 7.0.0 to 7.7.3 and 8.0.0 to 8.6.2 prevents some features considered dangerous (which could be used for remote code execution) to be configured in a ConfigSet that's uploaded via API without authentication/authorization. The checks in place to prevent such features can be circumvented by using a combination of UPLOAD/CREATE actions.

How it works

Successful exploitation of this vulnerability could lead to disclosure of sensitive information, addition or modification of data, or Denial of Service (DoS)

What to do

Be sure to have the appropriate security updates recommended by vendor

Reference

https://security.netapp.com/advisory/ntap-20201023-0002/

Heap-Based Buffer Overflow in Sudo *(CVE-2021-3156)* Severity: HIGH

Description

Sudo before 1.9.5p2 has a Heap-based Buffer Overflow, allowing privilege escalation to root via "sudoedit -s" and a command-line argument that ends with a single backslash character

1 CERT Tonga adopts the Traffic Light Protocol

How it works

A bug in the code that removes the escape characters will read beyond the last character of a string if it ends with an unescaped backslash character. Under normal circumstances, this bug would be harmless since sudo has escaped all the backslashes in the command's arguments. However, due to a different bug, this time in the command line parsing code, it is possible to run sudoedit with either the -s or -i options, setting a flag that indicates shell mode is enabled. Because a command is not actually being run, sudo does not escape special characters. Finally, the code that decides whether to remove the escape characters did not check whether a command is actually being run, just that the shell flag is set. This inconsistency is what makes the bug exploitable.

What to do

Users and administrators to update to sudo version 1.9.5p2, refer to vendors for available patches.

Reference

https://www.sudo.ws/alerts/unescape_overflow.html

Prisma Cloud Compute: SAML Authentication Bypass Vulnerability in Console *(CVE-2021-3033)* Severity: **HIGH**

Description

An improper verification of cryptographic signature vulnerability exists in the Palo Alto Networks Prisma Cloud Compute console.

How it works

This vulnerability enables an attacker to bypass signature validation during SAML authentication by logging in to the Prisma Cloud Compute console as any authorized user. This issue impacts: All versions of Prisma Cloud Compute 19.11, Prisma Cloud Compute 20.04, and Prisma Cloud Compute 20.09; Prisma Cloud Compute 20.12 before update 1. Prisma Cloud Compute SaaS version is not impacted by this vulnerability.

What to do

You can mitigate the impact of this issue by disabling SAML authentication in the Prisma Cloud Compute configuration

Reference

https://security.paloaltonetworks.com/CVE-2021-3033

Remote Code Execution Vulnerability in SAP Commerce Cloud *(CVE-2021-21477)* Severity: **HIGH**

Description

A remote code execution that exists in SAP Commerce Cloud

How it works

SAP Commerce Cloud, versions - 1808,1811,1905,2005,2011, enables certain users with required privileges to edit drools rules, an authenticated attacker with this privilege will be able to inject malicious code in the drools rules which when executed leads to Remote Code Execution vulnerability enabling the attacker to compromise the underlying host enabling him to impair confidentiality, integrity and availability of the application.

What to do

Be sure to apply the appropriate security updates recommended by vendor

Reference

https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=568460543

Remote Code Execution Vulnerability in Python *(CVE-2021-3177)* Severity: **HIGH**

Description

A vulnerability exists in Python

How it works

Python 3.x through 3.9.1 has a buffer overflow in PyCArg_repr in _ctypes/callproc.c, which may lead to remote code execution in certain Python applications that accept floating-point numbers as untrusted input, as demonstrated by a 1e300 argument to c_double.from_param. This occurs because sprintf is used unsafely.

What to do

Apply the appropriate security updates as recommended by the Vendor.

Reference

https://bugs.python.org/issue42938

HPE Moonshot Provisioning Manager Stack-based Overflow Vulnerability *(CVE-2021-25139)*

Severity: **HIGH**

Description

A potential security vulnerability has been identified in the HPE Moonshot Provisioning Manager v1.20.

How it works

The HPE Moonshot Provisioning Manager is an application that is installed in a VMWare or Microsoft Hyper-V environment that is used to setup and configure an HPE Moonshot 1500 chassis. This vulnerability could be remotely exploited by an unauthenticated user to cause a stack based buffer overflow using user supplied input to the `khuploadfile.cgi` CGI ELF. The stack-based buffer overflow could lead to Remote Code Execution, Denial of Service, and/or compromise system integrity.

What to do

HPE recommends that customers discontinue the use of the HPE Moonshot Provisioning Manager.
The HPE Moonshot Provisioning Manager application is discontinued, no longer supported, is not available to download from the HPE Support Center, and no patch is available.

Reference

https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04084en_us

SQL Injection Vulnerability in SonicWall SSL VPN *(CVE-2021-20016)* Severity: **HIGH**

Description

A SQL-Injection vulnerability in the SonicWall SSLVPN SMA100

How it works

A SQL-Injection vulnerability in the SonicWall SSLVPN allows a remote unauthenticated attacker to perform SQL query to access username password and other session related information. This vulnerability impacts SMA100 build version 10.x.

What to do

Ensure to appropriate security updates recommended by vendor

Reference

https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0001

Remote Code Execution Vulnerability in Apache Druid *(CVE-2021-25646)* Severity: **HIGH**

Description

A vulnerability that exist in Apache Druid

How it works

Apache Druid includes the ability to execute user-provided JavaScript code embedded in various types of requests. This functionality is intended for use in high-trust environments, and is disabled by default. However, in Druid 0.20.0 and earlier, it is possible for an authenticated user to send a specially-crafted request that forces Druid to run user-provided JavaScript code for that request, regardless of server configuration. This can be leveraged to execute code on the target machine with the privileges of the Druid server process.

What to do

Be sure to appropriate security updates recommended by the vendor

Reference

https://lists.apache.org/thread.html/rfeb775822cd3baef1595b60f6860f5ca849eb1903236483f3297bd5c@%3Ccommits.druid.apache.org%3E

Weak Authentication Vulnerability in Bosch Products Database *(CVE-2020-17530)* Severity: **HIGH**

Description

A vulnerability found in Bosch Products Database

How it works

Use of Hard-coded Credentials in the database of Bosch FSM-2500 server and Bosch FSM-5000 server up to and including version 5.2 allows an unauthenticated remote attacker to log into the database with admin-privileges. This may result in complete compromise of the confidentiality and integrity of the stored data as well as a high availability impact on the database itself. In addition, an attacker may execute arbitrary commands on the underlying operating system.

What to do

Ensure that you apply the most appropriate updates recommended by Vendor

Reference

https://psirt.bosch.com/security-advisories/BOSCH-SA-332072-BT.html

Microsoft Exchange Server Remote Code Execution Vulnerability *(CVE-2020-16875)* Severity: **HIGH**

Description

A remote code execution vulnerability exists in Microsoft Exchange server due to improper validation of cmdlet arguments.

How it works

An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the System user, aka 'Microsoft Exchange Server Remote Code Execution Vulnerability'.

.

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-2020-16875

Cisco Smart Software Manager Satellite Web UI Command Injection Vulnerabilities *(CVE-2021-1138, CVE-2021-1140, CVE-2021-1142)* Severity: **HIGH**

Description

Multiple vulnerabilities in the web UI of Cisco Smart Software Manager Satellite could allow an unauthenticated, remote attacker to execute arbitrary commands on the underlying operating system.

How it works

These vulnerabilities are due to insufficient input validation. An attacker could exploit these vulnerabilities by sending malicious HTTP requests to an affected device. A successful exploit could allow the attacker to run arbitrary commands on the underlying operating system.

What to do

Cisco has released software updates that address these vulnerabilities.

Reference

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cssm-multici-pgG5WM5A

Microsoft Defender Remote Code Execution Vulnerability *(CVE-2021-1647)* Severity: **HIGH**

Description

This vulnerability exists in Microsoft's Defender antivirus software. Attackers can write specially crafted files that can be run immediately when Microsoft Defender initiates the scans.

How it works

Attackers can use this vulnerability not only to bypass Microsoft anti-virus software but also to use Microsoft anti-virus software to run malicious software to launch an attack. This means that an attacker can launch a non-interactive attack, such as sending a specially crafted file as an email attachment, and the email client will trigger a scan after receiving it.

What to do

Ensure to apply appropriate security updates recommended by vendor

Reference

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1647

Arbitrary Code Execution Vulnerability in Flatpak *(CVE-2021-21261)* Severity: **HIGH**

Description

Flatpak is a system for building, distributing, and running sandboxed desktop applications on Linux. This vulnerability in the `flatpak-portal` service can allow sandboxed applications to execute arbitrary code on the host system (a sandbox escape).

How it works

This sandbox-escape bug is present in versions from 0.11.4 and before fixed versions 1.8.5 and 1.10.0. The Flatpak portal D-Bus service (`flatpak-portal`, also known by its D-Bus service name `org.freedesktop.portal.Flatpak`) allows apps in a Flatpak sandbox to launch their own subprocesses in a new sandbox instance, either with the same security settings as the caller or with more restrictive security settings. In vulnerable versions, the Flatpak portal service passes caller-specified environment variables to non-sandboxed processes on the host system, and in particular to the `flatpak run` command that is used to launch the new sandbox instance. A malicious or compromised Flatpak app could set environment variables that are trusted by the `flatpak run` command, and use them to execute arbitrary code that is not in a sandbox.

What to do

Ensure to apply appropriate security updates recommended by vendor

Reference

https://www.debian.org/security/2021/dsa-4830

IBM Security Identity Governance and Intelligence Missing Authentication *(CVE-2020-4958)*

Severity: **HIGH**

Description

IBM has announced a release for IBM Security Identity Governance and Intelligence (IGI) in response to security vulnerability. The vulnerability is due to the RMI connectors that do not appear to be authenticated.

How it works

IBM Security Identity Governance Virtual Appliance does not perform any authentication for functionality that requires a provable user identity or consumes a significant amount of resources.

What to do

Apply the most appropriate updates recommended by IBM

Reference

https://www.ibm.com/support/pages/node/6403247

Remote Code Execution Vulnerability in SolarWinds *(CVE-2021-25274)* Severity: **HIGH**

Description

The Collector Service in SolarWinds Orion Platform before 2020.2.4 uses MSMQ (Microsoft Message Queue) and doesn't set permissions on its private queues

How it works

As a result, remote unauthenticated clients can send messages to TCP port 1801 that the Collector Service will process. Additionally, upon processing of such messages, the service deserializes them in insecure manner, allowing remote arbitrary code execution as LocalSystem.

What to do

Ensure that you have the most appropriate security updates recommended by SolarWinds.

Reference

https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/full-system-control-with-new-solarwinds-orion-based-and-serv-u-ftp-vulnerabilities/

Hyper-V Remote Code Execution Vulnerability *(CVE-2020-17095)* Severity: **HIGH**

Description

A remote code execution vulnerability exists when Windows Hyper-V on a host server fails to properly validate input from an authenticated user on a guest operating system

How it works

To exploit this vulnerability, an attacker could run a specially crafted application on a Hyper-V guest that could cause the Hyper-V host operating system to execute arbitrary code when it fails to properly validate vSMB packet data.

What to do

Apply the most appropriate security updates recommended by Microsoft.

Reference

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2020-17095

Privilege Escalation Vulnerability in McAfee Web Gateway *(CVE-2021-23885)* Severity: **HIGH**

Description

This exploit requires the attacker to gain authenticated access to the MWG User Interface. McAfee recommends that access to the User Interface is restricted to trusted networks and that the number of people authorized to log on is limited. This issue results in commands being executed as root on the MWG appliance.

How it works

Privilege escalation vulnerability in McAfee Web Gateway (MWG) prior to 9.2.8 allows an authenticated user to gain elevated privileges through the User Interface and execute commands on the appliance via incorrect improper neutralization of user input in the troubleshooting page.

What to do

Apply the most appropriate security updates recommended by McAfee.

Reference

https://kc.mcafee.com/corporate/index?page=content&id=SB10349

Other Vulnerabilities with known Exploits

Unauthorized Access to SAP Provisioning Manager Software (*CVE-2021-21472)* Severity: **MEDIUM**

Description: Description: SAP Software Provisioning Manager 1.0 (SAP NetWeaver Master Data Management Server 7.1) does not have an option to set password during its installation, this allows an authenticated attacker to perform various security attacks like Directory Traversal, Password Brute force Attack, SMB Relay attack, Security Downgrade.

IBM QRadar SIEM Deserialization of Untrusted Data (*CVE-2020-4888)* Severity: **MEDIUM**

Description: IBM QRadar SIEM 7.4.0 to 7.4.2 Patch 1 and 7.3.0 to 7.3.3 Patch 7 could allow a remote attacker to execute arbitrary commands on the system, caused by insecure deserialization of user-supplied content by the Java deserialization function. By sending a malicious serialized Java object, an attacker could exploit this vulnerability to execute arbitrary commands on the system

XML Entity Expansion Vulnerability in Apache XMLBeans (*CVE-2021-23926)* Severity: **MEDIUM**

Description: This vulnerability exists in XML parsers used by XMLBeans up to version 2.6.0. The XML parsers did not set the properties needed to protect the user from malicious XML input. Hence, the resulting vulnerabilities include possibilities for XML Entity Expansion attacks.

Unauthenticated RCE Vulnerability in Oracle WebLogic Server (*CVE-2020-14882)* Severity: **MEDIUM**

Description: Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Console). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. 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.

Denial of Service Vulnerability in shttpd (*CVE-2021-26843)* Severity: **MEDIUM**

Description: Description: This is an issue in sthttpd through 2.27.1. On systems where the strcpy function is implemented with memcpy, the de_dotdot function may cause a Denial-of-Service (daemon crash) due to overlapping memory ranges being passed to memcpy. This can be triggered with an HTTP GET request for a crafted filename.

Arbitrary File Upload Vulnerability in Fortilogger (*CVE-2021-3378)* Severity: **MEDIUM**

Description: FortiLogger 4.4.2.2 is affected by Arbitrary File Upload by sending a "Content-Type: image/png" header to Config/SaveUploadedHotspotLogoFile and then visiting Assets/temp/hotspot/img/logohotspot.asp.

Cisco Connected Mobile Experiences Privilege Escalation Vulnerability *(CVE-2021-1144*) Severity: **MEDIUM**

Description: A vulnerability in Cisco Connected Mobile Experiences (CMX) could allow a remote, authenticated attacker without administrative privileges to alter the password of any user on an affected system. The vulnerability is due to incorrect handling of authorization checks for changing a password. An authenticated attacker without administrative privileges could exploit this vulnerability by sending a modified HTTP request to an affected device. A successful exploit could allow the attacker to alter the passwords of any user on the system, including an administrative user, and then impersonate that user.

Weak password requirements in SAP Software Provisioning Manager *(CVE-2021-21472*) Severity: **MEDIUM**

Description: SAP Software Provisioning Manager 1.0 (SAP NetWeaver Master Data Management Server 7.1) does not have an option to set password during its installation, this allows an authenticated attacker to perform various security attacks like Directory Traversal, Password Brute force Attack, SMB Relay attack, Security Downgrade.

Weak password requirements in SAP Software Provisioning Manager *(CVE-2020-35128*) Severity: **MEDIUM**

Description: Mautic before 3.2.4 is affected by stored XSS. An attacker with permission to manage companies, an application feature, could attack other users, including administrators. For example, by loading an externally crafted JavaScript file, an attacker could eventually perform actions as the target user. These actions include changing the user passwords, altering user or email addresses, or adding a new administrator to the system.

Improper Input Validation Vulnerability in SAP 3D VEV *(CVE-2021-21463*) Severity: **MEDIUM**

Description: SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated PCX file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation.

Other Vulnerabilities

Heap Buffer Overflow Vulnerability in Skia *(CVE-2021-21113)* Severity: **MEDIUM**

Description: Heap buffer overflow in Skia in Google Chrome prior to 87.0.4280.141 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.

OS Command Injection Vulnerability in Async-Git *(CVE-2021-3190)* Severity: **MEDIUM**

Description: The async-git package before 1.13.2 for Node.js allows OS Command Injection via shell Meta characters, as demonstrated by git.reset and git.tag.

Compiled with information from SANS' @RISK: The Consensus 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