TLP: White[1]

Security Bulletin – March 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

Microsoft Exchange Server Remote Code Execution Vulnerability (Proxylogon) *(CVE-2021-26855)* Severity: **HIGH**

Description

This is a Server-Side Request Forgery (SSRF) vulnerability that allows attackers to send arbitrary HTTP requests and authenticate to on-premise Exchange server.

How it works

It allows an unauthenticated attacker to send arbitrary HTTP requests and authenticate as the Exchange Server. The vulnerability exploits the Exchange Control Panel (ECP) via a Server-Side Request Forgery (SSRF). This would also allow the attacker to gain access to mailboxes and read sensitive information.

What to do

Be sure to have the appropriate security updates recommended by vendor

Reference

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26855

https://www.cert.gov.to/wp-content/uploads/2021/03/Advisory-for-on-Microsoft-Exchange-Supplement.pdf

1 CERT Tonga adopts the Traffic Light Protocol

Microsoft Exchange Server Remote Code Execution Vulnerability *(CVE-2021-26857)*

Severity: **HIGH**

Description

This is an insecure deserialization vulnerability in the Unified Messaging service.

How it works

Insecure deserialization is where untrusted user-controllable data is deserialized by a program. Attackers who successfully exploit this vulnerability can run their code as SYSTEM on the Exchange server.

What to do

Apply the most appropriate security update as recommended by Microsoft.

Reference

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-26857

Microsoft Exchange Server Remote Code Execution Vulnerability *(CVE-2021-26858)*

Severity: **HIGH**

Description

It is a post-authentication arbitrary file write vulnerability in Exchange.

How it works

This vulnerability is part of an attack chain. The initial attack requires the ability to make an untrusted connection to Exchange server port 443. Exploiting this vulnerability could allow an attacker to write a file to any part of the target Exchange server. Attackers exploiting this vulnerability could write a file to any path on the target Exchange server.

What to do

Apply the most appropriate security update as recommended by Microsoft.

Reference

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26858

Remote Code Execution Vulnerability in Genivia gSOAP *(CVE-2020-13576)* Severity: **HIGH**

Description

A code execution vulnerability exists in the WS-Addressing plugin functionality of Genivia gSOAP 2.8.107

How it works

The gSOAP toolkit is a C/C++ library for developing XML-based web services. It includes several plugins to support the implementation of SOAP and web service standards. The framework also provides multiple deployment options including modules for both IIS and Apache, standalone CGI scripts and its own standalone HTTP service.

A specially crafted SOAP request can lead to remote code execution. An attacker can send an HTTP request to trigger this vulnerability.

What to do

Ensure to apply the appropriate security updates recommended by vendor

Reference

https://talosintelligence.com/vulnerability_reports/TALOS-2020-1187

Command Injection Vulnerability in Samba Client *(CVE-2021-27185)* Severity: **HIGH**

Description

The samba-client package before 4.0.0 for Node.js allows command injection because of the use of process.exec

How it works

A malicious actor will be able to use this to inject malicious commands in the server hosting the Node JS application. This issue may lead to remote code execution if a client of the library calls the vulnerable method with untrusted input.

What to do

Apply the appropriate security updates as recommended by the Vendor.

Reference

https://advisory.checkmarx.net/advisory/CX-2021-4302

Unrestricted Path Traversal Vulnerability in Kubernetes Client *(CVE-2021-20218)*
Severity: **HIGH**

Description

A flaw was found in the fabric8 kubernetes-client in version 4.2.0 and after.

How it works

This flaw allows a malicious pod/container to cause applications using the fabric8 kubernetes-client `copy` command to extract files outside the working path. The highest threat from this vulnerability is to integrity and system availability. This has been fixed in kubernetes-client-4.13.2 kubernetes-client-5.0.2 kubernetes-.

What to do

Apply the most appropriate updates as recommended by the Vendor.

Reference

https://bugzilla.redhat.com/show_bug.cgi?id=1923405

https://access.redhat.com/security/cve/cve-2021-20218

Arbitrary Code Execution Vulnerability in Netgear Orbi Routers *(CVE-2020-27861)*

Severity: **HIGH**

Description

A vulnerability found in Netgear Orbi Routers

How it works

This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of NETGEAR Orbi 2.5.1.16 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the UA_Parser utility. A crafted Host Name option in a DHCP request can trigger execution of a system call composed from a user-supplied string. An attacker can leverage this vulnerability to execute code in the context of root.

What to do

It is recommended that you keep your NETGEAR devices up to date with the latest firmware.

Firmware updates contain security fixes, bug fixes, and new features for your NETGEAR products.

Reference

https://kb.netgear.com/000062507/Security-Advisory-for-Unauthenticated-Command-Injection-Vulnerability-on-Some-Extenders-and-Orbi-WiFi-Systems-PSV-2020-0301

Cisco Application Services Engine Unauthorized Access Vulnerabilities *(CVE-2021-1393)* Severity: **HIGH**

Description

Multiple vulnerabilities in Cisco Application Services Engine

How it works

It could allow an unauthenticated, remote attacker to gain privileged access to host-level operations or to learn device-specific information, create diagnostic files, and make limited configuration changes.

What to do

Be sure to appropriate security updates recommended by the vendor

Reference

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-case-mvuln-dYrDPC6w

Remote Code Execution in SpringBoot Framework *(CVE-2021-26987)* Severity: **HIGH**

Description

A vulnerability found in SpringBoot Framework

How it works

Element Plug-in for vCenter Server incorporates SpringBoot Framework. SpringBoot Framework versions prior to 1.3.2 are susceptible to a vulnerability which when successfully exploited could lead to Remote Code Execution. All versions of Element Plug-in for vCenter Server, Management Services versions prior to 2.17.56 and Management Node versions through 12.2 contain vulnerable versions of SpringBoot Framework.

What to do

Ensure that you apply the most appropriate updates that is recommended by Vendor

Reference

https://security.netapp.com/advisory/ntap-20210315-0001/

Vulnerabilities found in Accellion *(CVE-2021-27101, CVE- 2021-27102, CVE-2021-27103, CVE-2021-27104, CVE-2021-27730)* Severity: **HIGH**

Description

There has been multiple vulnerabilities found in Accellion products

How it works

Actors have exploited the vulnerabilities to attack multiple federal and state, local, tribal, and territorial (SLTT) government organizations as well as private industry organizations including those in the medical, legal, telecommunications, finance, and energy sectors. According to Accellion, this activity involves attackers leveraging multiple vulnerabilities to target FTA customers.

What to do

Ensure that you apply the most appropriate updates that is recommended by Accellion

Reference

https://www.accellion.com/products/fta/

Unauthorized Authentication Vulnerability in Cisco MSO *(CVE-2021-1388)* Severity: **HIGH**

Description

A vulnerability in an API endpoint of Cisco ACI Multi-Site Orchestrator (MSO) installed on the Application Services Engine.

How it works

It could allow an unauthenticated, remote attacker to bypass authentication on an affected device. The vulnerability is due to improper token validation on a specific API endpoint. An attacker could exploit this vulnerability by sending a crafted request to the affected API. A successful exploit could allow the attacker to receive a token with administrator-level privileges that could be used to authenticate to the API on affected MSO and managed Cisco Application Policy Infrastructure Controller (APIC) devices

What to do

Ensure to apply appropriate security updates recommended by CISCO

Reference

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-mso-authbyp-bb5GmBQv

Unauthenticated Access Vulnerability in Oracle WebLogic Server *(CVE-2021-2047)*

Severity: **HIGH**

Description

This vulnerability is in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core Components). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, and 12.2.1.3.0.

How it works

Easily exploitable vulnerability allows unauthenticated attacker with network access via IIOP, T3 to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server

What to do

Ensure to apply appropriate security updates recommended by vendor

Reference

https://www.oracle.com/security-alerts/cpujan2021.html

Server Side Template Injection Vulnerability in Saltstack *(CVE-2021-25283)* Severity: **HIGH**

Description

An issue was discovered in through SaltStack Salt before 3002.5.

How it works

The jinja renderer does not protect against server-side template injection attacks.

What to do

Apply the most appropriate updates recommended by the Vendor

Reference

https://saltproject.io/security_announcements/active-saltstack-cve-release-2021-feb-25/

Remote Un-authentication Vulnerability in Saltstack *(CVE-2021-25281)* Severity: **HIGH**

Description

An issue was discovered in through SaltStack Salt before 3002.5. salt-api does not honor eauth credentials for the wheel_async client. Thus, an attacker can remotely run any wheel modules on the master.

How it works

salt-api does not honor eauth credentials for the wheel_async client. Thus, an attacker can remotely run any wheel modules on the master.

What to do

Update to the latest Salt release, package or patch file

Reference

https://saltproject.io/security_announcements/active-saltstack-cve-release-2021-feb-25/

Shell Injection Vulnerability in SaltStack *(CVE-2021-3197)* Severity: **HIGH**

Description

An issue was discovered in SaltStack Salt before 3002.5.

How it works

The salt-api's ssh client is vulnerable to a shell injection by including ProxyCommand in an argument, or via ssh_options provided in an API request.

What to do

Apply the most appropriate security updates recommended by Vendor

Reference

https://saltproject.io/security_announcements/active-saltstack-cve-release-2021-feb-25/

Command Injection Vulnerability in SaltStack *(CVE-2021-3148)* Severity: **HIGH**

Description

An issue was discovered in SaltStack Salt before 3002.5. Sending crafted web requests to the Salt API can result in salt.utils.thin.gen_thin() command injection because of different handling of single versus double quotes. This is related to salt/utils/thin.py.

How it works

A remote attacker could possibly execute arbitrary commands via salt-api, cause a Denial of Service condition, bypass access restrictions or disclose sensitive information.

What to do

Apply the most appropriate security updates recommended by Vendor and make sure to update to the latest version.

Reference

https://saltproject.io/security_announcements/active-saltstack-cve-release-2021-feb-25/

Other Vulnerabilities with known Exploits

Double-Free Memory Corruption Vulnerability in OpenSSH (CVE-2021-28041**)**

Severity: **MEDIUM**

Description: ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.

SQL Injection Vulnerability in HGiga Mail (*CVE-2021-22848)* Severity: **MEDIUM**

Description: HGiga MailSherlock contains a SQL Injection. Remote attackers can inject SQL syntax and execute SQL commands in a URL parameter of email pages without privilege.

Authentication Bypass Vulnerability in WP Plugin (*CVE-2021-24148)* Severity: **MEDIUM**

Description: A business logic issue in the Store API WordPress plugin, versions before 3.2.0, had an authentication bypass with Sign In With Apple allowing unauthenticated users to recover an authentication cookie with only an email address

Improper Memory Read Vulnerability in Google Chrome (*CVE-2021-21150)* Severity: **MEDIUM**

Description: Use after free in Downloads in Google Chrome on Windows prior to 88.0.4324.182 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.

Command Injection Vulnerability in Docker Dashboard (*CVE-2021-27886)* Severity: **MEDIUM**

Description: rakibtg Docker Dashboard before 2021-02-28 allows command injection in backend/utilities/terminal.js via shell metacharacters in the command parameter of an API request. NOTE: this is NOT a Docker, Inc. product.

OS Command Injection in SolarView Compact (*CVE-2021-20658)* Severity: **MEDIUM**

Description SolarView Compact SV-CPT-MC310 prior to Ver.6.5 allows an attacker to execute arbitrary OS commands with the web server privilege via unspecified vectors.

Other Vulnerabilities

Deserialization Vulnerability in IntelliJ Idea (*CVE-2021-25758)* Severity: **MEDIUM**

Description: In JetBrains IntelliJ IDEA before 2020.3, potentially insecure deserialization of the workspace model could lead to local code execution.

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

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