TLP: White[1]

Security Bulletin – August 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 SonicWall Analytics *(CVE-2021-20032)*

Severity: **HIGH**

Description

SonicWall Analytics 2.5 On-Prem is vulnerable to Java Debug Wire Protocol (JDWP)

How it works

There was a security misconfiguration vulnerability which potentially leads to Remote Code Execution. This vulnerability impacts Analytics On-Prem 2.5.2518 and earlier.

What to do

SonicWall strongly recommends that administrators block access to 9000/TCP port on affected versions.

Reference

https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0018

Remote Code Execution Vulnerability in Cisco IP Phones *(CVE-2020-3161)* Severity: **HIGH**

Description

A vulnerability in the web server for Cisco IP Phones could allow an unauthenticated, remote attacker to execute code with root privileges or cause a reload of an affected IP phone, resulting in a denial of service (DoS) condition.

1 CERT Tonga adopts the Traffic Light Protocol

How it works

The vulnerability is due to a lack of proper input validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web server of a targeted device. A successful exploit could allow the attacker to remotely execute code with root privileges or cause a reload of an affected IP phone, resulting in a DoS condition.

What to do

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

Reference

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-voip-phones-rce-dos-rB6EeRXs

Missing Authorization Vulnerability in Citrix ShareFile *(CVE-2021-22891)* Severity:

HIGH

Description

A missing authorization vulnerability exists in Citrix ShareFile Storage Zones Controller before 5.7.3, 5.8.3, 5.9.3, 5.10.1 and 5.11.18

How it works

This may allow unauthenticated remote compromise of the Storage Zones Controller.

What to do

Apply the most appropriate updates as recommended by the Vendor.

Reference

https://support.citrix.com/article/CTX310780

Remote Code Execution Vulnerability in Lucee Server *(CVE-2021-21307)* Severity:

HIGH

Description

Lucee Server is a dynamic, Java based (JSR-223), tag and scripting language used for rapid web application development.

How it works

In Lucee Admin before versions 5.3.7.47, 5.3.6.68 or 5.3.5.96 there is an unauthenticated remote code exploit.

What to do

This is fixed in versions 5.3.7.47, 5.3.6.68 or 5.3.5.96. As a workaround, one can block access to the Lucee Administrator.

Reference

https://dev.lucee.org/t/lucee-vulnerability-alert-november-2020/7643

Malicious File Upload Vulnerability in Apache Commons *(CVE-2020-1953)* Severity: **HIGH**

Description

Apache Commons Configuration uses a third-party library to parse YAML files which by default allows the instantiation of classes if the YAML includes special statements. Apache Commons Configuration versions 2.2, 2.3, 2.4, 2.5, 2.6 did not change the default settings of this library.

How it works

An unauthenticated attacker can have the YAML file was loaded from an untrusted source, it could therefore load and execute code out of the control of the host application.

What to do

Apply the appropriate security updates as recommended by the Vendor.

Reference

https://lists.apache.org/thread.html/rde2186ad6ac0d6ed8d51af7509244adcf1ce0f9a3b7e1d1dd3b64676@%3Ccommits.camel.apache.org%3E

Remote Desktop Client Remote Code Execution Vulnerability *(CVE-2021-34535)*

Severity: **HIGH**

Description

The vulnerability exists in the latest Serv-U version 15.2.3 HF1 released May 5, 2021, and all prior versions

How it works

A threat actor who successfully exploited this vulnerability could run arbitrary code with privileges. An attacker could then install programs; view, change, or delete data; or run programs on the affected system

What to do

Apply the most appropriate updates as recommended by Solarwinds

Reference

https://www.solarwinds.com/trust-center/security-advisories/cve-2021-35211

Deserialization Vulnerability in Apache OFBiz *(CVE-2021-29200)* Severity: **HIGH**

Description

Apache OFBiz has unsafe deserialization prior to 17.12.07 version

How it works

An unauthenticated user can perform an RCE attack

What to do

Upgrade to at least 17.12.07 or apply one of the patches at https://issues.apache.org/jira/browse/OFBIZ-12216

Reference

https://lists.apache.org/thread.html/re21d25d9fb89e36cea910633779c23f144b9b60596b113b7bf1e8097@%3Cuser.ofbiz.apache.org%3E

Remote Desktop Client Remote Code Execution Vulnerability *(CVE-2021-34535)*

Severity: **HIGH**

Description

This vulnerability occurs in the client, not in the server.

How it works

For exploitation to occur, victims would need to be lured to a server controlled by an attacker or be exposed to a malicious program in a guest virtual machine. On Hyper-V servers, a malicious program running in a guest VM could trigger guest-to-host RCE by exploiting this vulnerability in the Hyper-V Viewer.

What to do

Apply the most appropriate updates as recommended by the Microsoft.

Reference

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34535

Improper Authentication Vulnerability in Dell iDRAC9 *(CVE-2021-21538)* Severity:

HIGH

Description

Dell EMC iDRAC9 versions 4.40.00.00 and later, but prior to 4.40.10.00, contain an improper authentication vulnerability.

How it works

A remote unauthenticated attacker could potentially exploit this vulnerability to gain access to the virtual console.

What to do

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

Reference

https://www.dell.com/support/kbdoc/000186420

Remote Code Execution Vulnerability in Microsoft SMB (*CVE-2020-0796)* Severity:

HIGH

Description

A remote code execution vulnerability exists in the way that the Microsoft Server Message Block 3.1.1 (SMBv3) protocol handles certain requests, aka 'Windows SMBv3 Client/Server Remote Code Execution Vulnerability.

How it works

To exploit the vulnerability against a server, an unauthenticated attacker could send a specially crafted packet to a targeted SMBv3 server. To exploit the vulnerability against a client, an unauthenticated attacker would need to configure a malicious SMBv3 server and convince a user to connect to it.

What to do

Make sure to apply the appropriate security updates recommended by Microsoft

Reference

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0796

Other Vulnerabilities with known Exploits

Windows Update Medic Service Privilege Escalation Vulnerability (*CVE-2021-36948)*

Severity: **MEDIUM**

Description: The vulnerability is in Windows 10 and Server 2019 and newer operating systems with the Update Medic Service. Update Medic is a new service that allows users to repair Windows Update components from a damaged state such that the device can continue to receive updates. The exploit is both low complexity and can be exploited without user interaction, making this an easy vulnerability to include in an adversary's toolbox. This vulnerability has been seen exploited in the wild and it is crucial that organizations move quickly to patch and remediate this vulnerability.

Pulse Connect Secure RCE Patch Vuln (*CVE-2021-22937)* Severity: **MEDIUM**

Description: This is a post-authentication, distant codification execution (i.e., RCE) vulnerability that exists on Pulse Connect Secure virtual backstage web (i.e., VPN) appliances.It is a patch bypass for CVE-2020-8260 which was disclosed in Oct. 2020. CVE-2021-22937 is an uncontrolled archive extraction vulnerability in the Pulse Connect Secure appliance that allows an authenticated administrator to write arbitrary executable files. This unrestricted file upload vulnerability is due to a flaw in the way that archive files are extracted in the administrator web interface. Successful exploitation would give attackers root privileges on the targeted appliance.

Buffer Overflow Vulnerability in Tensorflow (*CVE-2020-15196)* Severity: **MEDIUM**

Description: In Tensorflow version 2.3.0, the `SparseCountSparseOutput` and RaggedCountSparseOutput` implementations don't validate that the `weights` tensor has the same shape as the data. The check exists for `DenseCountSparseOutput`, where both tensors are fully specified. In the sparse and ragged count weights are still accessed in parallel with the data. But, since there is no validation, a user passing fewer weights than the values for the tensors can generate a read from outside the bounds of the heap buffer allocated for the weights. The issue is patched in commit 3cbb917b4714766030b28eba9fb41bb97ce9ee02 and is released in TensorFlow version 2.3.1.

Weak Authentication Vulnerability in SAP Solution Manager (*CVE-2020-26821)*

Severity: **MEDIUM**

Description: SAP Solution Manager (JAVA stack), version - 7.20, allows an unauthenticated attacker to compromise the system because of missing authorization checks in the SVG Converter Service, this has an impact to the integrity and availability of the service.

Weak Authentication Vulnerability in IBM Security Guardium (*CVE-2021-20418)*

Severity: **MEDIUM**

Description: IBM Security Guardium 11.2 does not require that users should have strong passwords by default, which makes it easier for attackers to compromise user accounts. IBM X-Force ID: 196279.

Buffer Overflow Vulnerability in Broadcom Brocade Fabric OS *(CVE-2020-15373)*

Severity: **MEDIUM**

Description: Multiple buffer overflow vulnerabilities in REST API in Brocade Fabric OS versions v8.2.1 through v8.2.1d, and 8.2.2 versions before v8.2.2c could allow remote unauthenticated attackers to perform various attacks.

Weak Authentication Vulnerability in Schneider Electric Modicon PLC *(CVE-2017-6028)* Severity: **MEDIUM**

Description: An Insufficiently Protected Credentials issue was discovered in Schneider Electric Modicon PLCs Modicon M241, all firmware versions, and Modicon M251, all firmware versions. Log-in credentials are sent over the network with Base64 encoding leaving them susceptible to sniffing. Sniffed credentials could then be used to log into the web application.

Code Execution Vulnerability in Shader Functionality – AMD Radeon Directx Driver (*CVE-2020-6102)* Severity: **MEDIUM**

Description: An exploitable code execution vulnerability exists in the Shader functionality of AMD Radeon DirectX 11 Driver atidxx64.dll 26.20.15019.19000. An attacker can provide a specially crafted shader file to trigger this vulnerability, resulting in code execution. This vulnerability can be triggered from a HYPER-V guest using the RemoteFX feature, leading to executing the vulnerable code on the HYPER-V host (inside of the rdvgm.exe process). Theoretically this vulnerability could be also triggered from web browser (using webGL and webassembly).

Other Vulnerabilities

Improper Access Control Vulnerability in Rancher (*CVE-2021-25320)* Severity: **MEDIUM**

Description: An Improper Access Control vulnerability in Rancher, allows users in the cluster to make request to cloud providers by creating requests with the cloud-credential ID. Rancher in this case would attach the requested credentials without further checks. This issue affects: Rancher versions prior to 2.5.9; Rancher versions prior to 2.4.16.

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