Ministry of Meteorology Energy
Information, Disaster Management,
Environment, Communications and
Climate Change

TLP: White[1]

Security Bulletin – November 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 Oracle Secure Product Engineers Online Portal system (*CVE-2021-42669)* Severity: **HIGH**

Description

The Engineers Online Portal system has an uncontrolled file upload vulnerability.

How it works

An attacker can take advantage of this flaw to gain remote code execution on the vulnerable web server. When an avatar is submitted, it goes into the /admin/uploads/ directory, which is accessible to all users. The attacker can get remote code execution on the web server by submitting a simple PHP web shell.

What to do

Ensure that you apply the appropriate updates recommended.

Reference

https://www.sourcecodester.com/php/13115/engineers-online-portal-php.html

https://github.com/TheHackingRabbi/CVE-2021-42669

[1] CERT Tonga adopts the Traffic Light Protocol

Remote code execution vulnerability in Microsoft Virtual Machine Bus (VMBus) *(CVE-2021-26443)* Severity: **HIGH**

Description

Microsoft Virtual Machine Bus (VMBus) is a mechanism within the Hyper-V architecture that enables logical communication in partitions. The VMBus works as the internal communications channel to redirect requests to virtual devices, allowing files to be dragged and dropped between the virtual machine and the host.

This vulnerability occurs due to insufficient input validation in VMBus.

How it works

On the local network, a remote authenticated attacker can send a specially designed communication to the VMBus channel and run arbitrary code on the target system.

What to do

Apply the appropriate updates as recommended by Vendor

Reference

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26443

Remote Code Execution vulnerability in Sitecore XP 7.5 *(CVE-2021-42237)* Severity: **HIGH**

Description

Sitecore Experience Platform (XP) is a marketing automation solution that carves out personalized customer experiences.

How it works

From Sitecore XP 7.5 Initial Release to Sitecore XP 8.2 Update-7, an unsafe deserialization attack makes it possible to execute remote commands on the machine.

To exploit this flaw, no authentication or specific setting is necessary.

What to do

In order to fix this vulnerability:

- For Sitecore XP 7.5.0 - Sitecore XP 7.5.2, use one of the following solutions:
- Upgrade your Sitecore XP instance to Sitecore XP 9.0.0 or higher.

Reference

https://support.sitecore.com/kb?id=kb_article_view&sysparm_article=KB1000776

Memory corruption vulnerability in Palo Alto Networks PAN-OS GlobalProtect Portal and Gateway *(CVE-2021-3064)* Severity: HIGH

Description

PAN-OS is the software that runs all Palo Alto Network's next-generation firewalls. The Palo Alto Networks Global Protect portal and gateway interfaces are susceptible to a memory corruption vulnerability.

How it works

It allows an unauthenticated network-based attacker to disrupt system processes and potentially execute arbitrary code with root capabilities.

To exploit this flaw, the attacker must have network access to the GlobalProtect interface.

This vulnerability affects PAN-OS 8.1 versions before 8.1.17 but does not affect Prisma Access customers.

What to do

Ensure that you apply the appropriate updates recommended.

Reference

https://security.paloaltonetworks.com/CVE-2021-3064

SQL injection vulnerability in the PHP Event Calendar (*CVE-2021-42077)* Severity: HIGH

Description

PHP Event Calendar is an AJAX-based, multi-user modern event calendar. It is easy to integrate and fully customizable.

The /server/ajax/user manager.php username parameter in PHP Event Calendar prior to 2021-09-03 allows SQL injection. This can be used to directly execute SQL statements on the database, allowing an attacker to entirely compromise the database system in some situations. It can also be used to avoid having to fill out the login form.

How it works

Due to improper validation, the application is vulnerable to SQL injection attacks. For example, the following SQL statement can be used as a username during the login process to bypass the authentication:

' OR '1' = '1' #

This vulnerability cannot only be exploited to bypass the login.

It can also be used to execute SQL statements directly on the database, allowing an adversary in some cases to completely compromise the database system.

What to do

Update to a recent version of PHP Event Calendar.

Reference

https://www.syss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2021-048.txt

Other Vulnerabilities with known Exploits

Remote code execution vulnerability in HSMX internet gateway (*CVE-2021-40521)*

Severity: **MEDIUM**

Description: The HSMX Gateway is a platform designed to manage authentication and billing in your network.

The device can be tricked into downloading and running a malicious package from a remote server controlled by the attacker, allowing the attacker to execute root-level code. When these holes are combined, an attacker may be able to get root access to the device.

Other Vulnerabilities

Improper Access Control in Emerson Devices (*CVE-2020-12030)* Severity: **MEDIUM**

Description: There is a flaw in the code used to configure the internal gateway firewall when the gateway's VLAN feature is enabled. If a user enables the VLAN setting, the internal gateway firewall becomes disabled resulting in exposure of all ports used by the gateway.

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