**TLP: White**[1]

# Security Bulletin – January 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

### Zend Framework Remote Code Execution Vulnerability *(CVE-2021-3007)* Severity: HIGH

**Description**

A remote code execution in Zend Framework

**How it works**

Zend Framework has a deserialization vulnerability that can lead to remote code execution if the content is controllable, related to the __destruct method of the Zend\Http\Response\Stream class in Stream.php.

**What to do**

Be sure to appropriate security updates recommended by vendor

**Reference**

https://github.com/laminas/laminas-http/commits/2.15.x/src/Response/Stream.php

### Zyxel Firewalls And AP Controller Hardcoded Credential Vulnerability *(CVE-2020-29583)* Severity: HIGH

**Description**

A vulnerability exists in Zyxel Firewalls and AP controllers.

**How it works**

Firmware version Zyxel USG devices contains an undocumented account (zyfwp) with an unchangeable password. The password for this account can be found in cleartext in the firmware. This account can be used by someone to login to the ssh server or web interface with admin privileges.

**What to do**

Apply the appropriate security updates recommended

1 CERT Tonga adopts the Traffic Light Protocol

### Reference

https://www.zyxel.com/support/security_advisories.shtml

## DNS Forwarder dnsmasq multiple Vulnerabilities *(CVE-2020-25681)* Severity: **HIGH**

### Description


Multiple vulnerabilities found in DNS forwarder

### How it works

A flaw was found in dnsmasq. A heap-based buffer overflow was discovered in the way RRSets are sorted before validating with DNSSEC data. An attacker on the network, who can forge DNS replies such as that they are accepted as valid, could use this flaw to cause a buffer overflow with arbitrary data in a heap memory segment, possibly executing code on the machine.

### What to do

Ensure to appropriate security updates recommended

### Reference

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/WYW3IR6APUSKOYKL5FT3ACTIHWHGQY32/

## FortiWeb Blind SQL Injection Vulnerability *(CVE-2020-29015)* Severity: **HIGH**

### Description

A vulnerability that exist in FortiWeb

### How it works

A blind SQL injection in the user interface of FortiWeb that may allow an unauthenticated, remote attacker to execute arbitrary SQL queries or commands by sending a request with a crafted Authorization header containing a malicious SQL statement.

### What to do

Be sure to appropriate security updates recommended by the vendor

### Reference

https://www.fortiguard.com/psirt/FG-IR-20-124

## Zyxel Hardcoded Credential Vulnerability *(CVE-2020-17530)* Severity: **HIGH**

### Description

A vulnerability found on Zyxel

### How it works

Zyxel USG devices contains an undocumented account (zyfwp) with an unchangeable password. The password for this account can be found in cleartext in the firmware. This account can be used by someone to login to the ssh server or web interface with admin privileges

### What to do

Ensure that you apply  the most appropriate updates recommended by Vendor

### Reference

https://businessforum.zyxel.com/discussion/5252/zld-v4-60-revoke-and-wk48-firmware-release

## Microsoft Windows NTFS Remote Code Execution Vulnerability *(CVE-2020-17096)* Severity: **HIGH**

### Description

Microsoft Windows is exposed to NTFS remote code execution vulnerability

### How it works

A local attacker could run a specially crafted application that would elevate the attacker's privileges. A remote attacker with SMBv2 access to a vulnerable system could send specially crafted requests over a network to exploit this vulnerability and execute code on the target 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-2020-17096

## Microsoft .Net Framework Remote Code Execution Injection Vulnerability *(CVE-2020-4606)* Severity: **HIGH**

### Description

A remote code execution vulnerability exists when the Microsoft .NET Framework fails to validate input properly

### How it works

An attacker who successfully exploited this vulnerability could take control of an affected system. To exploit the vulnerability, an attacker would need to pass specific input to an application utilizing susceptible .Net methods.

### What to do

Ensure to apply appropriate security updates recommended by vendor

### Reference

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0646

## Micro Focus ArcSight Logger Code Injection Vulnerability *(CVE-2020-11851)* Severity: **HIGH**

### Description

A vulnerability found on Micro Focus

### How it works

Arbitrary code execution vulnerability on Micro Focus ArcSight Logger product. The vulnerability could be remotely exploited resulting in the execution of arbitrary code.

### What to do

Apply the most appropriate security updates recommended by Micro Focus.

### Reference

https://community.microfocus.com/t5/Logger/Logger-Release-Notes-7-1-1/ta-p/2837600

## Other Vulnerabilities with known Exploits

## Apache Flink Directory Traversal Vulnerability (*CVE-2020-17519)* Severity: **MEDIUM**

Description: Apache Flink allows attackers to read any file on the local filesystem of the JobManager through the REST interface of the JobManager process. Access is restricted to files accessible by the JobManager process.

## Cisco ASA Remote File Disclosure Vulnerability (*CVE-2020-3452)* Severity: **MEDIUM**

Description: A vulnerability in the web services interface of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to conduct directory traversal attacks and read sensitive files on a targeted system. The vulnerability is due to a lack of proper input validation of URLs in HTTP requests processed by an affected device. An attacker could exploit this vulnerability by sending a crafted HTTP request containing directory traversal character sequences to an affected device

## Google Chrome Heap Corruption Vulnerability (*CVE-2020-16040)* Severity: **MEDIUM**

Description: Insufficient data validation in V8 in Google Chrome allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. The exploitation doesn't require any form of authentication. However, successful exploitation requires user interaction by the victim.

### **Oracle WebLogic Server Vulnerability (***CVE-2021-2109)* Severity: **MEDIUM**

Description: A vulnerability exists in the Oracle WebLogic Server product of Oracle Fusion Middleware. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server.

### **Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability (***CVE-2020-17136)* Severity: **MEDIUM**

Description: Microsoft Windows could allow a local authenticated malicious user to gain elevated privileges on the system, caused by a flaw in the Cloud Files Mini Filter Driver. By executing a specially-crafted program, an authenticated attacker could exploit this vulnerability to execute arbitrary code with higher privileges.

### **Missing Authentication Check in SAP Solution Manager (***CVE-2020-6207)* Severity: **MEDIUM**

Description: SAP Solution Manager (User Experience Monitoring), version- 7.2, due to Missing Authentication Check does not perform any authentication for a service resulting in complete compromise of all SMDAgents connected to the Solution Manager.

### **Cisco DNA Center Cross-Site Request Forgery Vulnerability** *(CVE-2021-1257*) Severity: **MEDIUM**

Description: A vulnerability in the web-based management interface of Cisco DNA Center Software could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack to manipulate an authenticated user into executing malicious actions without their awareness or consent. The vulnerability is due to insufficient CSRF protections for the web-based management interface of an affected device. An attacker could exploit this vulnerability by persuading a web-based management user to follow a specially crafted link. A successful exploit could allow the attacker to perform arbitrary actions on the device with the privileges of the authenticated user. These actions include modifying the device configuration, disconnecting the user's session, and executing Command Runner commands.

### **ECSIMAGING PACS 6.21.5 - SQL injection Vulnerability** *(CVE-2021-3118*) Severity: **MEDIUM**

Description: Unsupported versions of EVOLUCARE ECSIMAGING (aka ECS Imaging) products through 6.21.5 has multiple SQL Injection issues in the login form and the password-forgotten form. This allows an attacker to steal data in the database and obtain access to the application.

### **Improper method call validation allows arbitrary code execution vulnerability** *(CVE-2020-11651*) Severity: **MEDIUM**

Description: This vulnerability exists in SaltStack Salt before 2019.2.4 and 3000 before 3000.2. The salt-master process ClearFuncs class does not properly validate method calls. This allows a remote user to access some methods without

authentication. These methods can be used to retrieve user tokens from the salt master and/or run arbitrary commands on salt minions.

## Other Vulnerabilities

### Laravel in debug mode susceptible to Remote code execution vulnerability *(CVE-2021-3129)*

Severity: **MEDIUM**

Description: Ignition before 2.5.2, as used in Laravel and other products, allows unauthenticated remote attackers to execute arbitrary code because of insecure usage of file_get_contents() and file_put_contents() methods. This is exploitable on sites using debug mode with Laravel before 8.4.2.

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