



Click here to
sign-up

FortiGate

FortiGate
intelligence
performance

This Board

Cookie Settings

By clicking "Accept All", you are consenting to the use of cookies on your device to enhance site functionality, analyze site usage, and assist in our marketing efforts. This includes the use of cookies and similar technologies to show you personalized advertising on other websites through our partners. To accept only necessary cookies, select "Reject All." You can visit the [Cookie Settings](#) link, which contains details on specific cookies, categories, and preference options. Your choice will apply only to your current browser/device. Please also see our [Privacy Policy](#) for more information on how we process personal data. [privacy policy](#)

[Cookie Settings](#)

Reject All

Accept All



Carl_Windsor_FTNT

Staff

Created on

12-12-2022

09:08 PM

Edited on

12-20-2022

03:09 AM

By

MOD Jean-Philippe_P

Article

2394

Technical Tip: [Critical vulnerability] Protect against heap-based buffer overflow in sslvpnd

Description

This article describes how a critical heap-based buffer overflow vulnerability [CWE-122] in FortiOS SSL-VPN may allow a remote, unauthenticated attacker to execute arbitrary code or commands with specifically crafted requests. See the FortiGuard page on the vulnerability for more details: <https://www.fortiguard.com/psirt/FG-IR-22-398>

Scope

FortiGate.

Solution

Fortinet recommends taking immediate action to mitigate this vulnerability (by [disabling SSL VPN](#)) before upgrading to the latest release, as documented in the advisory.

If a FortiGate is managed by a FortiManager, ensure that the FortiManager is upgraded to a compatible version before upgrading the FortiGate. For more information, see the [FortiManager Compatibility Chart](#).

To search for the Crash Log indicators of compromise documented in the advisory, search the Event Logs either on the FortiGate or the FortiAnalyzer for multiple System level log events containing the following information:

```
Logdesc="Application crashed" and msg="[...] application: sslvpnd,[...], Signal 11  
received
```

Alternative

```
# diag
```

Search for

```
xxxx:  
xxxx:  
xxxx:
```

Cookie Settings

By clicking "Accept All", you are consenting to the use of cookies on your device to enhance site functionality, analyze site usage, and assist in our marketing efforts. This includes the use of cookies and similar technologies to show you personalized advertising on other websites through our partners. To accept only necessary cookies, select "Reject All." You can visit the [Cookie Settings](#) link, which contains details on specific cookies, categories, and preference options. Your choice will apply only to your current browser/device. Please also see our [Privacy Policy](#) for more information on how we process personal data. [privacy policy](#)

Additionally, search for the presence of the IoC artifacts in the filesystem with the fnsysctl command:

```
# fnsysctl ls -l /data/lib
```

```
/data/lib/liblips.bak  
/data/lib/libgif.so  
/data/lib/libiptcp.so  
/data/lib/libipudp.so  
/data/lib/libjpeg.so
```

```
# fnsysctl ls -la /var
```

```
/var/.sslvpnconfigbk
```

```
# fnsysctl ls -l /data/etc
```

```
/data/etc/wxd.conf
```

```
# fnsysctl ls -l /
```

```
/flash
```


If these IoCs are detected, contact customer support for assistance.


 48781

 | 10

[Submit Article Idea](#)

COMMENTS




crao 

Created On

This was

Cookie Settings

By clicking "Accept All", you are consenting to the use of cookies on your device to enhance site functionality, analyze site usage, and assist in our marketing efforts. This includes the use of cookies and similar technologies to show you personalized advertising on other websites through our partners. To accept only necessary cookies, select "Reject All." You can visit the Cookie Settings link, which contains details on specific cookies, categories, and preference options. Your choice will apply only to your current browser/device. Please also see our Privacy Policy for more information on how we process personal data. [privacy policy](#)



Contributors



Carl_Windsor_FTNT



Stephen_G



Anthony_E



Jean-Philippe_P



GusZ

Broad. Integrated. Automated.

The Fortinet Security Fabric brings together the concepts of convergence and consolidation to provide comprehensive cybersecurity protection for all users, devices, and applications and across all network edges.

Social Media



Cookie Settings

By clicking "Accept All", you are consenting to the use of cookies on your device to enhance site functionality, analyze site usage, and assist in our marketing efforts. This includes the use of cookies and similar technologies to show you personalized advertising on other websites through our partners. To accept only necessary cookies, select "Reject All." You can visit the Cookie Settings link, which contains details on specific cookies, categories, and preference options. Your choice will apply only to your current browser/device. Please also see our Privacy Policy for more information on how we process personal data. [privacy policy](#)

SECURITY

Threat Research

FortiGuard Labs

Threat Map

Threat Briefs

Ransomware

Getting Started Resources

Careers

Certifications

Events

Industry Awards

Social Responsibility

CONTACT US

Corporate

Community

Copyright 2024 Fortinet, Inc. All Rights Reserved.

[Terms of Service](#) | [Privacy Policy](#) | [GDPR](#) | [Cookie Settings](#)