Community

Help

Click here to sign-up

Forums Knowledge Base Community Groups Blogs

FortiGate

FortiGate Next Generation Firewall utilizes purpose-built security processors and threat intelligence security services from FortiGuard labs to deliver top-rated protection and high performance, including encrypted traffic.

This Board Sea

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

Fortinet Community > Knowle

Carl_Windsor_FTNT
Staff

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, Backtrace: [...]“
```

Alternatively, execute the following command on the FortiGate CLI:

```
# diagnose debug crashlog read
```

Search for multiple examples of the following:

```
xxxx: [ Date & Time ] <.....> firmware  [ Firmware version ]
xxxx: [ Date & Time ] <.....> application sslvpnd
xxxx: [ Date & Time ] <.....> *** signal 11 (Segmentation fault) received ***
```

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

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

/data/lib/libips.bak
/data/lib/libgif.so
/data/lib/libiptcp.so
/data/lib/libipudp.so
/data/lib/libjepg.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.

48791 10

Submit Article Idea

COMMENTS

crao
Staff

This was very useful. T

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

FORTINET Community

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

SECURITY RESEARCH	COMPANY	NEWS & ARTICLES
Threat Research	About Us	News Releases
FortiGuard Labs	Security Fabric	News Articles

Threat Map

Threat Briefs

Ransomware

Getting Started Resources

Exec. Mgmt

Careers

Certifications

Events

Industry Awards

Social Responsibility

Trademarks

CONTACT US

Corporate

Community