



Created on

12-12-2022 09:08 PM

Edited on

12-20-2022 03:09 AM

Ву

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 <u>disabling SSL VPN</u>) 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
recei

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

XXXX:

XXXX:

XXXX:

Additionally, search for the presence of the 10C artifacts in the mesystem with the msystir command:

fnsysctl ls -l /data/lib

/data/lib/libips.bak
/data/lib/libipif.so
/data/lib/libipitcp.so
/data/lib/libipidp.so
/data/lib/libjepg.so

fnsysctl ls -la /var

/var/.sslvpnconfigbk

fnsysctl ls -1 /data/etc

/data/etc/wxd.conf

fnsysctl ls -1 /

/flash

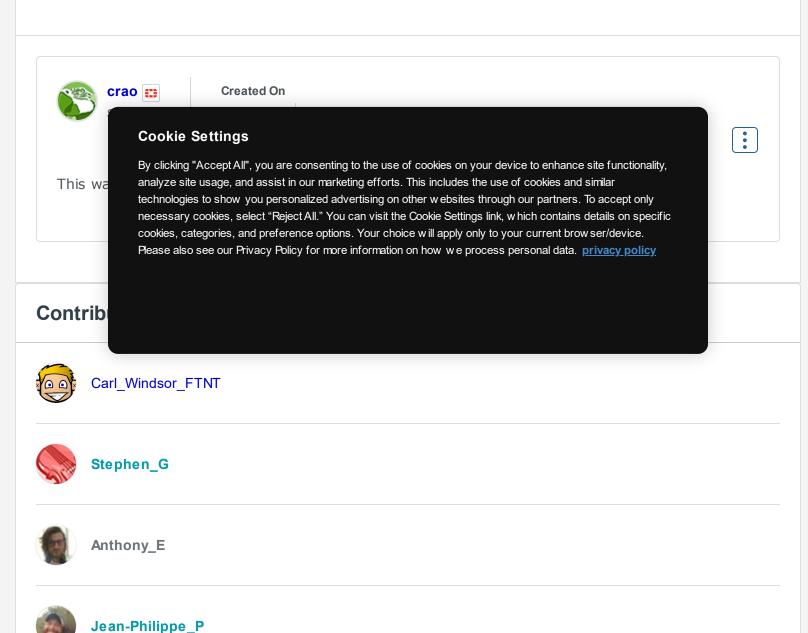
If these IoCs are detected, contact customer support for assistance.

48781



Submit Article Idea







GusZ

FERTINET. 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





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 brow ser/device. Please also see our Privacy Policy for more information on how we process personal data. <u>privacy policy</u>

S

Threat Resea

SECURITY

FortiGuard La

Threat Map

Threat Briefs Careers

Ransomware Certifications

Getting Started Resources Events Corporate

Industry Awards Community

Social Responsibility

Copyright 2024 Fortinet, Inc. All Rights Reserved.

Terms of Service | Privacy Policy | GDPR | Cookie Settings

Page 4 of 4