FortiOS SSL-VPN Buffer Overflow | CVE-2022-42475 / CVE-2023-27997

Overview

A FortiOS vulnerability was published on December 12, 2022 under the ID CVE-2022-42475. It describes a heap-based buffer overflow vulnerability [CWE-122] in FortiOS SSL-VPN. GE Gas Power has identified several of its own products that include an impacted FortiOS version, listed below.

An additional vulnerability was identified under the ID CVE-2023-27997 on June 12th, 2023, also impacting SSL-VPN. As this feature is not used on GE equipment, GE strongly recommends disabling this feature using the guidance provided in the "Remediation/Mitigation" section below.

Affected Products and Versions

GE Products:

- NetworkST4 (301E or 401E)
- Remote Operations Offering (101F)
- M&D Lockbox (60F)

FortiOS Versions:

- FortiOS version 7.2.0 through 7.2.4
- FortiOS version 7.0.0 through 7.0.11
- FortiOS version 6.4.0 through 6.4.12
- FortiOS version 6.2.0 through 6.2.13
- FortiOS 6.0 through 6.0.16
- FortiProxy version 7.2.0 through 7.2.3
- FortiProxy version 7.0.0 through 7.0.9
- FortiProxy version 2.0.0 through 2.0.12
- FortiProxy 1.2 all versions
- FortiProxy 1.1 all versions

Vulnerability Details

The vulnerability impacts FortiOS's SSL-VPN feature. If this service is enabled, a remote, unauthenticated attacker may be able to execute arbitrary code via specifically crafted requests.

Exploitation Status

Fortinet is aware of an instance where this vulnerability has been exploited in the field. GE Gas Power Product Security has not yet observed nor received reports of any exploit attempts against Gas Power Customers.

If a customer identifies that they are on an affected version of FortiOS, they should check for the following indicators of compromise before proceeding with mitigations. If any indicator of compromise is discovered, they should immediately raise an incident with GE. IOCs include:

Multiple log entries with:

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

Presence of the following artifacts in the filesystem:

/data/lib/libips.bak
/data/lib/libgif.so
/data/lib/libiptcp.so
/data/lib/libipudp.so
/data/lib/libjepg.so
/var/.sslvpnconfigbk
/data/etc/wxd.conf
/flash

Connections to suspicious IP addresses from the FortiGate:
188.34.130.40:444
103.131.189.143:30080,30081,30443,20443
192.36.119.61:8443,444
172.247.168.153:8033
139.180.184.197
66.42.91.32
158.247.221.101
107.148.27.117
139.180.128.142
155.138.224.122
185.174.136.20

Remediation/Mitigation

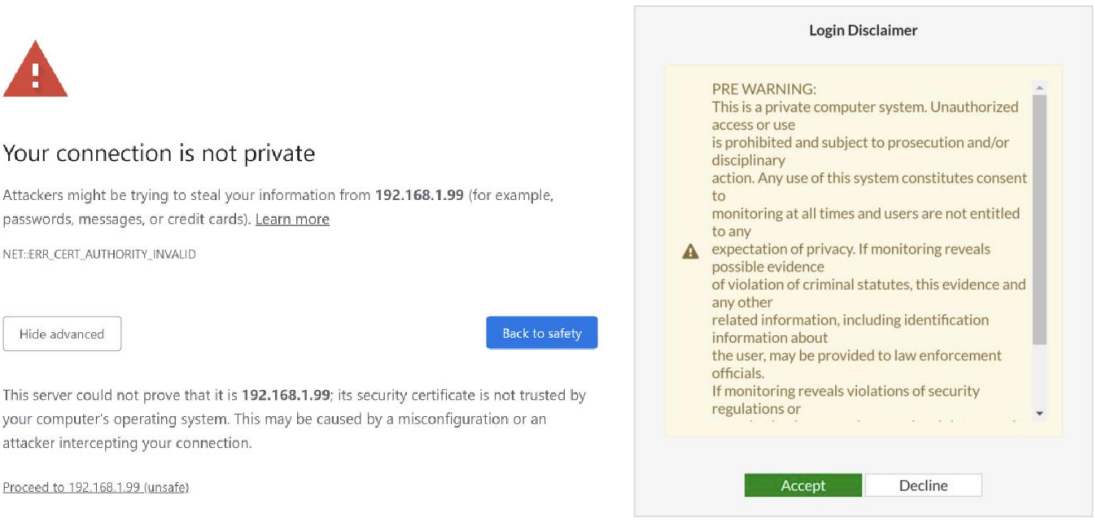
There are two ways to address this issue. One is to disable the feature through the firewall configuration; GE's architecture does not rely on this feature to operate. The other option is to update the firewall firmware. For this, you will need to contact your GE CPM and schedule an engagement. You will also need an active FortiOS subscription to perform the update. GE recommends the first option as it is cheaper, less disruptive and reduces future attack surface.

If you have Network ST4 and/or GE's Remote Operations solution deployed at site and you wish to change your configuration, you should follow the procedure below for the corresponding Fortinet firewalls.

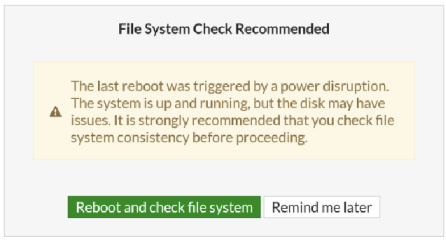
If your site has a 60F device as a part of your Monitoring and Diagnostics infrastructure, no action is required. GE has remotely deployed this workaround and disabled the SSL VPN on your device.

To disable the SSL VPN feature:

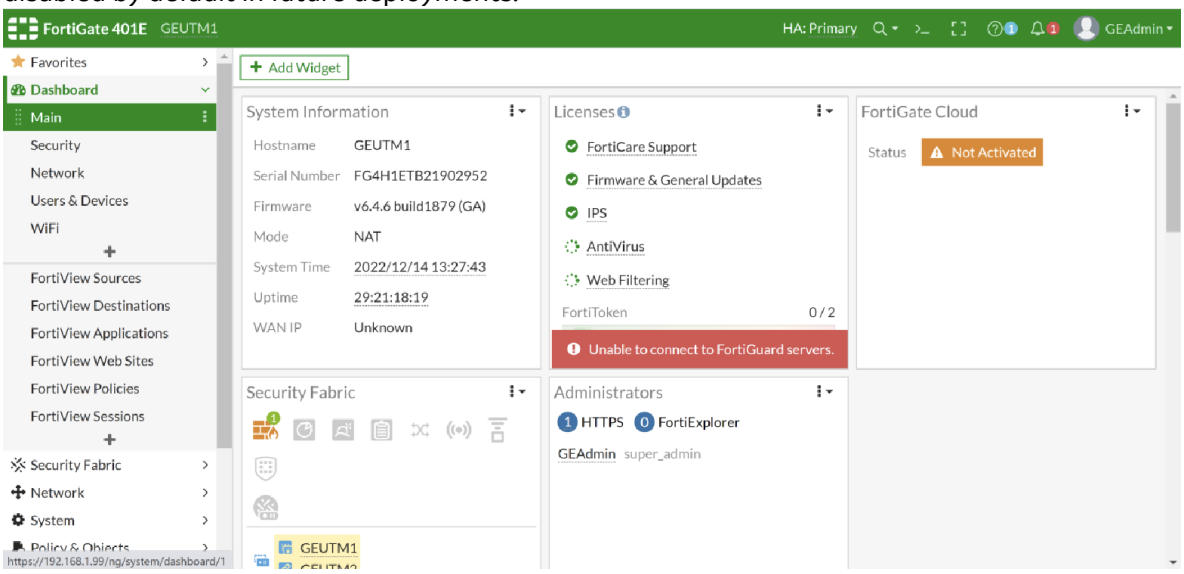
1) Log into UTM Firewall using MGMT Port. You will need to Accept the certificate warning and login disclaimer.



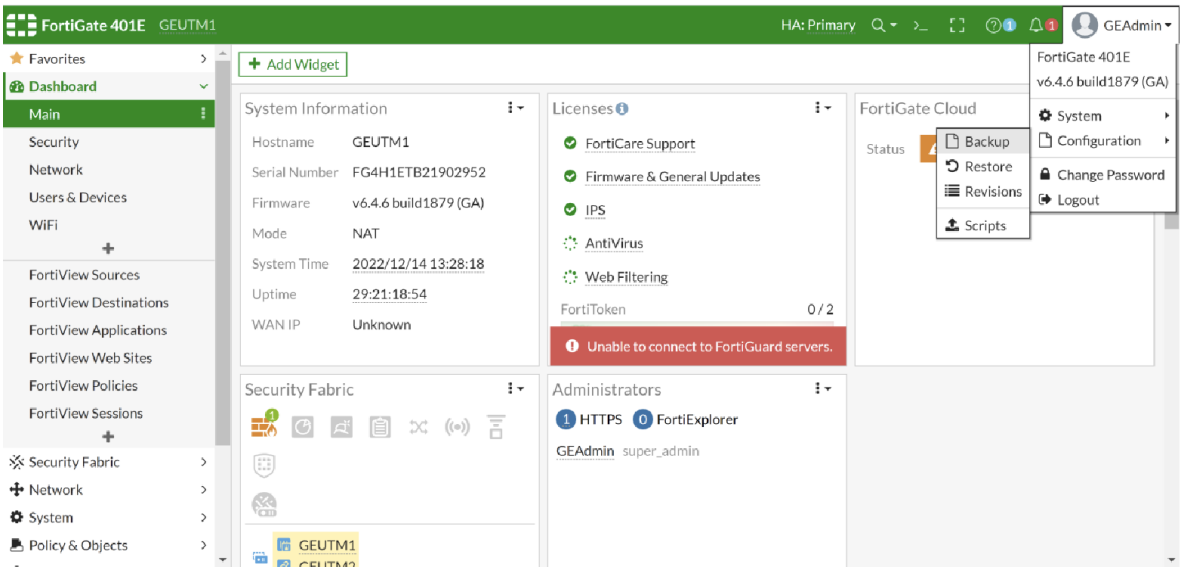
2) Enter login credentials and select “Remind me later”



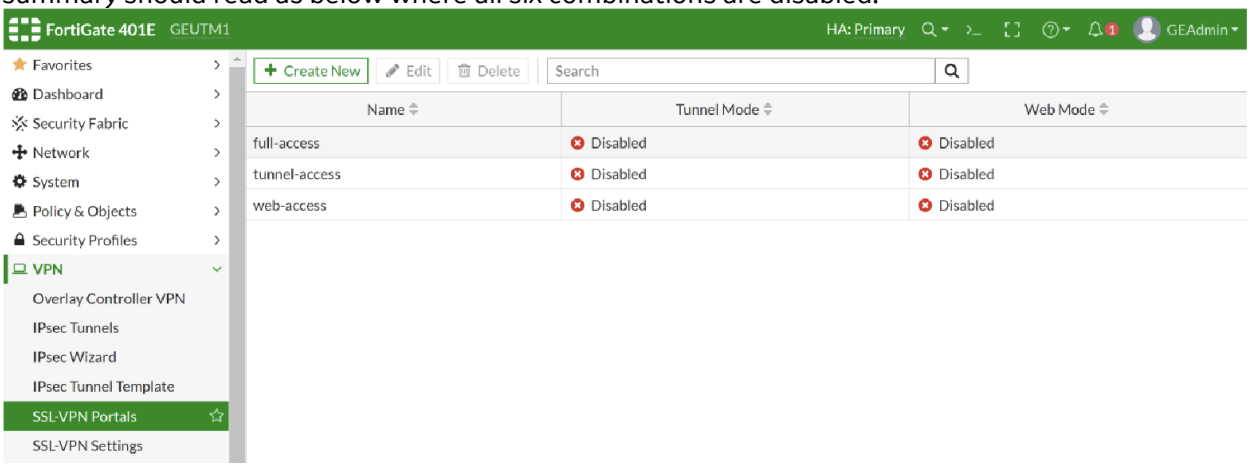
3) Check Firmware Version on the Main Dashboard. If you are using one of the affected versions, you should proceed with the remaining steps and check for IOCs described in the Exploitation Status section above. If you are not using one of the affected versions, GE Gas Power would still recommend you complete this process as the service is not necessary and will be disabled by default in future deployments.



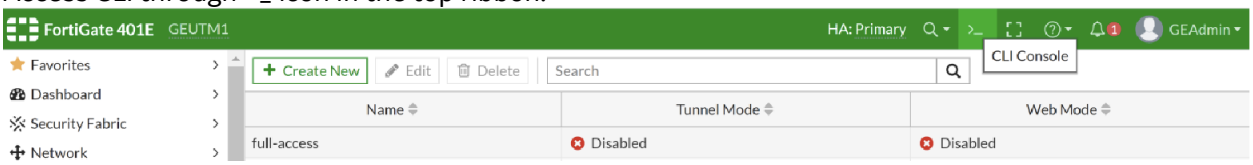
4) Create a backup by selecting the username and in the top right corner of the interface and then Configuration -> Backup. Confirm the backup was successful before proceeding.



5) In the sidebar, go to VPN -> SSL-VPN Portals and disable all features. When complete, the summary should read as below where all six combinations are disabled.



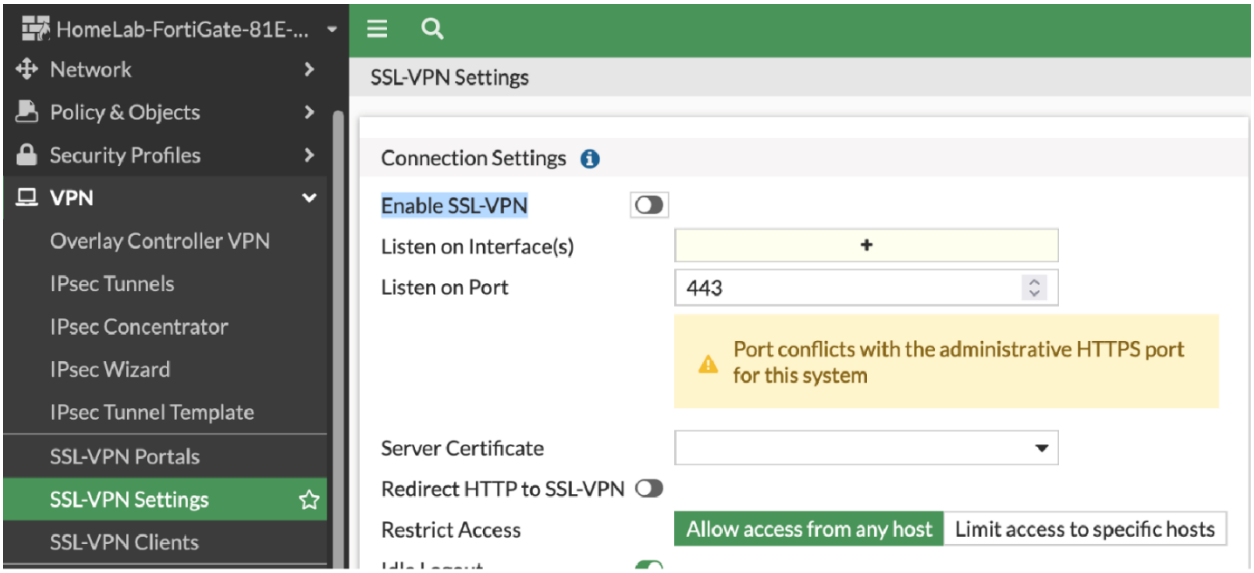
6) Disable SSL-VPN Service via CLI Interface (attempts to do so through GUI will result in errors). Access CLI through >_ icon in the top ribbon.



7) Enter for the following commands:

config vpn ssl settings
set status disable
end

8) Confirm the setting has been changed by opening SSL-VPN Settings in the GUI and ensuring the toggle is in the disabled position as below.



For additional information on the procedure or if any of these options don't seem to match your management interface, please refer to Fortinet's guide:

- https://community.fortinet.com/t5/FortiGate/Technical-Tip-nbsp-How-to-disable-SSL-VPN-functionality-on/ta-p/230801

Contact Information

Contact your local GE Services representative for assistance or for additional information.
For Product Security issues or incident/vulnerability reporting: www.ge.com/power/cybersecurity

Document History

Version	Release Date	Purpose
1.0	2/10/2023	Initial Release
2.0	6/22/2023	Added CVE-2023-27997 information