FortiOS - Format String Bug in HTTPSd | CVE-2023-36639

Overview

A FortIOS vulnerability was published on December 12, 2023 under the ID CVE-2023-36639 and Fortinet FG-IR-23-138. It describes a format string vulnerability [CWE-134] in the HTTPSd daemon of FortiOS, FortiProxy, and FortiPAM, which may allow an authenticated user to execute unauthorized code or commands via specially crafted API requests.

Severity

The vendor has set the severity of this issue with a CVSSv3 score of 7.2 (High).

Affected Products and Versions

GE Vernova Products with affected firmware:

- NetworkST4 (301E or 401E)
- Remote Operations Offering (101E/F)

Impacted FortiOS Versions:

Version	Affected	Solution
FortiOS 7.2	7.2.0 through 7.2.4	Upgrade to 7.2.6
FortiOS 7.0	7.0.0 through 7.0.11	Upgrade to 7.0.12 or above
FortiOS 6.4	6.4.0 through 6.4.12	Upgrade to 6.4.13 or above
FortiOS 6.2	6.2.0 through 6.2.15	Upgrade to 6.2.16 or above
FortiOS 6.0	6.0 all versions	Migrate to a fixed release

Vulnerability Details

A use of externally controlled format string in Fortinet allows attacker to execute code or commands via specially crafted API requests.

Exploitation Status

Fortinet internally discovered and reported by Fortinet Product Security team in the frame of an internal audit of the SSL-VPN component. GE Vernova Product Security has not yet observed nor received reports of any exploit attempts against Vernova Customers.

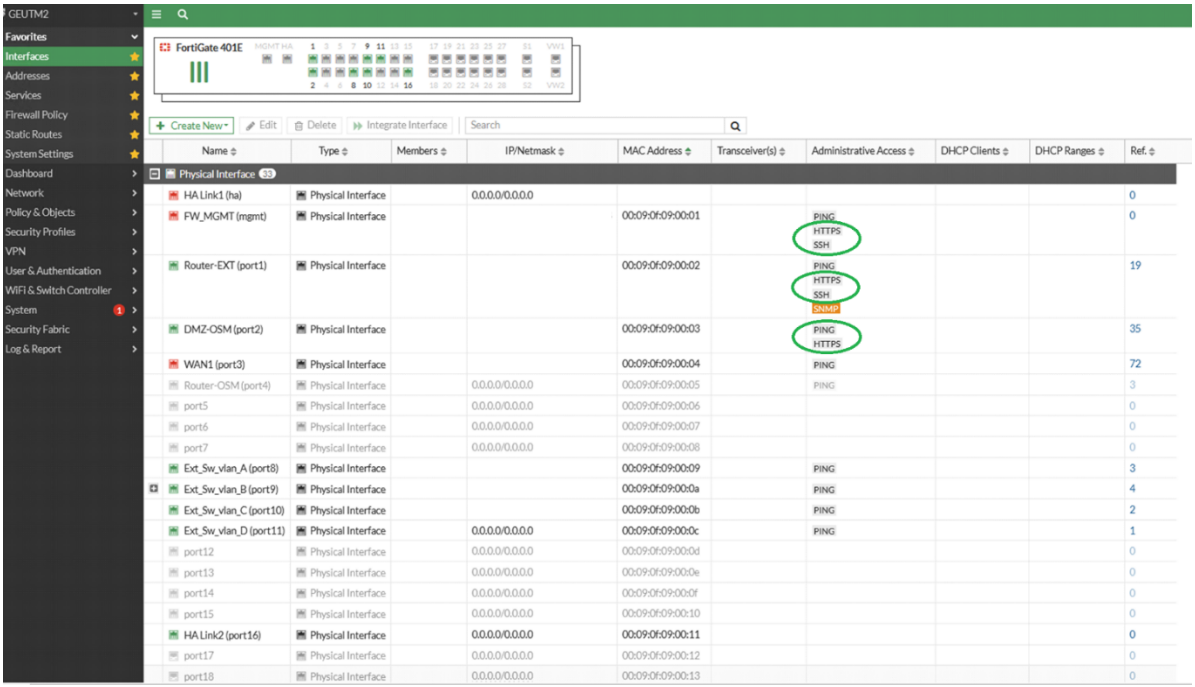
If a customer identifies that they are on an affected version of FortiOS, they should perform the following to assist with mitigation as an immediate response and upgrade the firmware as soon as possible. If any indicator of compromise is discovered, they should immediately raise an incident with GE Vernova.

Remediation

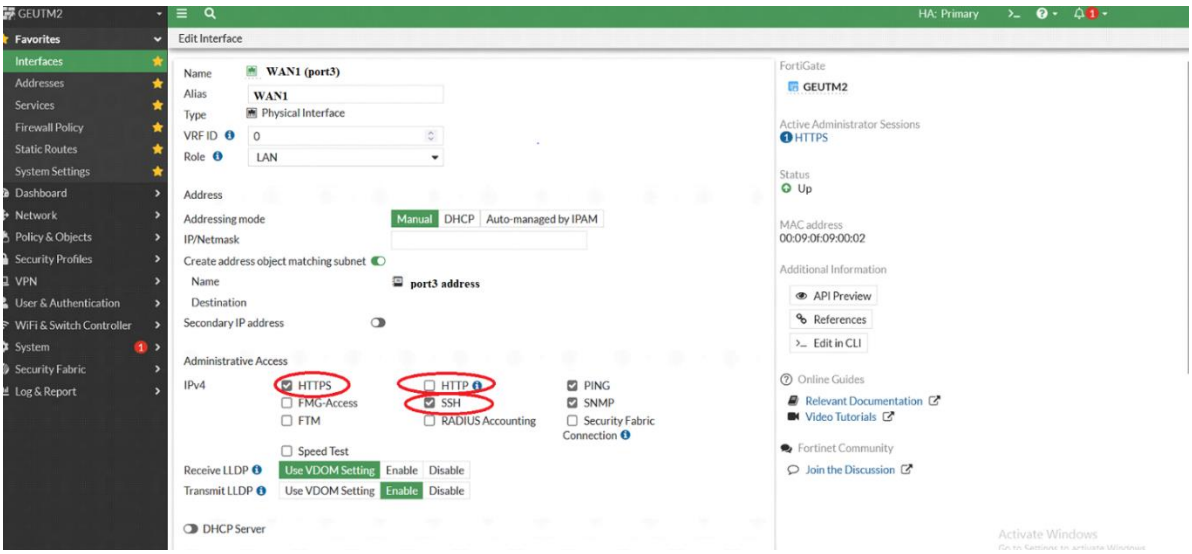
GE Vernova has completed validation of FortiOS v7.2.6 for the impacted products listed above and recommends updating to this version to resolve this vulnerability. If the firmware cannot be updated immediately, there are additional mitigation steps listed in the next section.

Mitigation

Remove HTTP, HTTPS and SSH access from interface ports which are external facing of the GE Controls network and does NOT require administrative access. The following interfaces MGMT, Port1, and port2 provide the functionality for administrative access (in the screenshot below). If HTTP, HTTPS and SSH is enabled on Port3 defined as a WAN port, this must be removed unless otherwise defined by the customer's security administration team.



As an example below, the WAN1(port3) had HTTPs and SSH enabled, select the port from the screen above and then remove the selections for the below highlighted (in red) services. Select OK and this will immediately modify the running and saved configuration.



Contact Information

Contact your local GE Services representative for assistance or for additional information.
For Product Security issues or incident/vulnerability reporting: https://www.ge.com/gas-power/products/digital-and-controls/cybersecurity

Document History

Version	Release Date	Purpose
1.0	02/05/2024	Initial Release