National Cyber Security Centre

202303081500-NCSC

A part of the **Department of the Environment, Climate & Communications**

# NCSC Alert

## FortiOS / FortiProxy - Heap buffer underflow in administrative interface allowing remote code execution

Thursday 9th March, 2023

**STATUS:** TLP-CLEAR

*Recipients can spread this to the world, there is no limit on disclosure. Sources may use* TLP-CLEAR *when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules,* TLP-CLEAR *information may be shared without restriction.* For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. Please treat this document in accordance with the TLP assigned.

## Description

Internal investigators at FortiNet have uncovered a vulnerability, CVE-2023-25610 in FortiOS/ FortiProxy that exploits a buffer underflow vulnerability to execute arbitrary code on the device and/or perform a DoS on the GUI, via specifically crafted requests.

FortiNet have released a patch, and detailed a work around on their advisory at https://www.fortiguard.com/psirt/FG-IR-23-001. They note that CVE-2023-25610 was discovered internally, and have not observed threat actors exploiting it.

The NCSC recommends that constituents using the FortiOS or FortiProxy devices assess their exposure to the risk and apply the risk mitigation provided by FortiNet as appropriate and in accordance with local change management policy.

## Products Affected

The advisory lists vulnerable software versions, and provides a list of devices. It notes that there are two risks from the vulnerability, those of remote code execution and DoS. All devices running the vulnerable software are at risk, but the devices listed are only vulnerable to the DoS risk, not both. If your device is not on the list but is running a vulnerable software version, it means that it is vulnerable to both risks.

- FortiOS version 7.2.0 through 7.2.3
- FortiOS version 7.0.0 through 7.0.9
- FortiOS version 6.4.0 through 6.4.11
- FortiOS version 6.2.0 through 6.2.12
- FortiOS 6.0 all versions
- FortiProxy version 7.2.0 through 7.2.2
- FortiProxy version 7.0.0 through 7.0.8
- FortiProxy version 2.0.0 through 2.0.11
- FortiProxy 1.2 all versions
- FortiProxy 1.1 all versions:

## Impact

Exploitation of CVE-2023-25610 may allow an remote unauthenticated attacker using crafted requests to:

- Execute remote coded on device
- Perform Denial of Service to use device GUI

## Recommendations

System managers should assess if their device is vulnerable to CVE-2023-25610, then check if the device type is listed in the advisory to assess if it is at exposed to both risks.

FortiNet have released updates for vulnerable systems, and identified version numbers in their advisory.

They have provided a details of a workaround that system managers should consider implementing while conducting change management on the device.

The core concept of the workaround is limiting the IP addresses allowed to access the GUI or disabling the GUI completely.

## References


- https://www.fortiguard.com/psirt/FG-IR-23-001 FortiNet advisory
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-25610 CVE details, placeholder as at time of publication.

**DISCLAIMER:** This document is provided “as is” without warranty of any kind, expressed or implied, including, but not limited to, the implied warranty of fitness for a particular purpose. NCSC-IE does not endorse any commercial product or service, referenced in this document or otherwise.

National Cyber Security Centre
29-31 Adelaide Road,
Dublin, D02 X285,
Ireland
**Tel:** +353 (0)1 6782333
**Mail:** certreport@decc.gov.ie
**Web:** ncsc.gov.ie
**Twitter:** ncsc_gov_ie
**LinkedIn:** ncsc-ie