National Cyber Security Centre

2403150128-NCSC

Department of the Environment, Climate & Communications

NCSC Alert

Critical Vulnerabilities exist in Fortinet FortiOS, FortiProxy CVE-2023-42789, CVE-2023-42790 (CVSSv3: 9.3)

Friday 15th March, 2024

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

Published: 2024-03-12T15:15:00
Vendor: Fortinet
Product: FortiOS, FortiProxy

CVE ID: CVE-2023-42789
CVSS3.0 Score[1]**:** 9.3
Summary: A out-of-bounds write in Fortinet FortiOS, FortiProxy captive portal allows attacker to execute unauthorised code or commands via specially crafted HTTP requests.

CVE ID: CVE-2023-42790
CVSS3.0 Score: 9.3
Summary: A stack-based buffer overflow in Fortinet FortiOS, FortiProxy captive portal allows attacker to execute unauthorised code or commands via specially crafted HTTP requests.

More information related to this issue including a workaround can be found at the following link(s):
https://fortiguard.fortinet.com/psirt/FG-IR-23-328

Products Affected

Fortinet FortiOS, FortiProxy

- FortiOS version 7.4.0 through 7.4.1
- FortiOS version 7.2.0 through 7.2.5
- FortiOS version 7.0.0 through 7.0.12
- FortiOS version 6.4.0 through 6.4.14
- FortiOS version 6.2.0 through 6.2.15
- FortiProxy version 7.4.0
- FortiProxy version 7.2.0 through 7.2.6
- FortiProxy version 7.0.0 through 7.0.12
- FortiProxy version 2.0.0 through 2.0.13

Impact

Common Weakness Enumeration (CWE)[2]**:** Execute unauthorised code or commands

Present in CISA Known Exploited Vulnerability(KEV)[3] **catalog:** NO
Used by Ransomware Operators: Not Known

[1] https://www.first.org/cvss/v3.0/specification-document
[2] https://cwe.mitre.org/
[3] https://www.cisa.gov/known-exploited-vulnerabilities-catalog

Recommendations

The NCSC strongly advises affected organisations to review the latest release notes and install the relevant updates from Fortinet.

Additional recommendations and mitigation's including a workaround for CVE-2023-42789 and CVE-2023-42790 can be found in the respective link(s) below:
https://fortiguard.fortinet.com/psirt/FG-IR-23-328

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@ncsc.gov.ie
Web: ncsc.gov.ie
Twitter: ncsc_gov_ie
LinkedIn: ncsc-ie