National Cyber Security Centre

2306120168-NCSC

Department of the Environment, Climate & Communications

NCSC Alert

Critical Vulnerability in FortiOS and FortiProxy SSL-VPN devices (CVE-2023-27997)

Tuesday 13th June, 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.

Revision History

Revision	Date	Author(s)	Description
1.0	12 June 2023	CSIRT-IE	Initial advisory responding to Fortinet warning
1.1	13 June 2023	CSIRT-IE	Update with detail from Fortinet

Description

Fortinet has disclosed information about a heap-based buffer overflow vulnerability in FortiOS and FortiProxy SSL-VPN. The vulnerability may allow a remote attacker to execute arbitrary code or commands via specifically crafted requests. The vulnerability was patched in an update released on 9th June 2023.

Weaknesses in firewalls are attractive to threat actors. Threat Actors exploited previous vulnerabilities in Fortinet devices within days of their official disclosure.

The Fortinet disclosure withheld technical details regarding CVE-2023-27997 to protect clients, and to slow the weaponisation of the vulnerability by threat actors.

Products Affected

FortiOS-6K7K

- FortiOS-6K7K version 7.0.10
- FortiOS-6K7K version 7.0.5
- FortiOS-6K7K version 6.4.12
- FortiOS-6K7K version 6.4.10
- FortiOS-6K7K version 6.4.8
- FortiOS-6K7K version 6.4.6
- FortiOS-6K7K version 6.4.2
- FortiOS-6K7K version 6.2.9 through 6.2.13
- FortiOS-6K7K version 6.2.6 through 6.2.7
- FortiOS-6K7K version 6.2.4
- FortiOS-6K7K version 6.0.12 through 6.0.16
- FortiOS-6K7K version 6.0.10

FortiProxy

- 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

FortiOS

- 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 version 6.0.0 through 6.0.16

Impact

Exploitation of this vulnerability could allow an unauthenticated, remote attacker to execute arbitrary code or commands via specifically crafted requests.

Fortinet have withheld technical detail on CVE-2023-27997. As a result, it is not possible to provide a definitive analysis on the full potential impact.

Fortinet have reported in a blog that CVE-2023-27997 may have been exploited in a "limited number of cases" to date and they are working with affected customers.

Recommendations

The NCSC recommends that affected devices are patched to the latest versions where applicable. Organisations that are unable to patch should anticipate exploitation of the vulnerability and plan accordingly.

If an organisation is not operating SSL-VPN, the risk of this issue is mitigated – however, Fortinet still advise to upgrade to the recommended versions.

Update advice is included in the Fortinet advisory: https://www.fortiguard.com/psirt/FG-IR-23-097

In addition to the immediate upgrading of systems, we advise implementing the recommendations in this FortiOS 7.2.0 Hardening Guide: https://docs.fortinet.com/document/fortigate/7.2.0/best-practices/555436/hardening

We also recommend that any organisation running affected appliances should engage with their FortiNet representative, if they have not done so already.

Sources

- Talos™ Cyber Veille Fortinet FortiGate VPN-SSL: https://olympecyberdefense.fr/1193-2/
- Researcher Charles Fol: https://twitter.com/cfreal_/status/1667852157536616451
- Mitre CVE: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-27997
- Fortinet disclosure: https://www.fortiguard.com/psirt/FG-IR-23-097
- Fortinet blog: https://www.fortinet.com/blog/psirt-blogs/analysis-of-cve-2023-27997-and-clarifications-on-volt-typhoon-campaign

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