National Cyber Security Centre

20230713-NCSC

Department of the Environment, Climate & Communications

NCSC Alert

Fortinet Releases Security update for critical vulnerability CVE-2023-33308

Thursday 13th July, 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

Fortinet has released a security update to address a critical vulnerability (CVE-2023-33308) affecting FortiOS and FortiProxy. This vulnerability allows a remote attacker to execute arbitrary code or commands via crafted packets reaching proxy policies or firewall policies with proxy mode alongside SSL deep packet inspection.

Fortinet's advisory can be found here https://www.fortiguard.com/psirt/FG-IR-23-183 and it is advised that constituents using impacted versions examine Fortinet's advice and take action to mitigate the vulnerability.

Products Affected

- FortiOS version 7.2.0 through 7.2.3
- FortiOS version 7.0.0 through 7.0.10
- FortiProxy version 7.2.0 through 7.2.2
- FortiProxy version 7.0.0 through 7.0.9

Impact

Exploitation of CVE-2023-33308 allows remote attackers to exploit a stack-based overflow vulnerability, allowing a remote attacker to perform arbitrary code execution on vulnerable devices.

Recommendations

Fortinet have released patches for CVE-2023-33308, https://www.fortiguard.com/psirt/FG-IR-23-183 which also details a potential workaround for this vulnerability with a sample configuration included with their advisory.

The workaround disables HTTP/2 support on SSL inspection profiles used by proxy policies or firewall policies with proxy mode. Details on this feature can be found at: `https://docs.fortinet.com/document/fortigate/7.0.0/new-features/710924/http-2-support-in-proxy-mode-ssl-inspection`

It is advised that constituents using impacted versions examine the advice from Fortinet and take actions to mitigate the vulnerability.

Threat groups attempt to weaponise disclosed vulnerabilities in a network perimeter device to conduct attacks.

Organisations should ensure that network devices are patched before vulnerabilities are weaponised.

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