National Cyber Security Centre

2210071906-NCSC

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

NCSC Alert

Critical Vulnerabilities in FortiOS, FortiSwitchManager and FortiProxy
CVE-2022-40684 (UPDATE 1.1)

11 October 2022

Status: TLP-WHITE

Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP-WHITE *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-WHITE *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	07 October 2022	CSIRT-IE	Initial Alert created
1.1	11 October 2022	CSIRT-IE	Alert updated to include details of Fortinet's public advisory

Description

Fortinet has released a critical software update[1] for FortiOS, FortiSwitchManager and FortiProxy, that addresses CVE-2022-40684, an authentication bypass on the administration interface. The security flaw could allow remote threat actors to perform operations on unpatched devices via specially crafted HTTP or HTTPS requests. The vulnerability has a **CVSSv3 Score of 9.6**.

Products Affected

- FortiOS: 7.0.0 to 7.0.6
- FortiOs: 7.2.0 to 7.2.1
- FortiProxy: From 7.0.0 to 7.0.6 and 7.2.0
- FortiSwitchManager: 7.0.0, 7.2.0

Impact

Remote Code Execution, access to sensitive data

Detection

Fortinet is aware of an instance where this vulnerability was exploited, and recommends immediately validating your systems against the following indicator of compromise in the device's logs:

```
user="Local_Process_Access"
```

Recommendations

The NCSC strongly advises affected organisations to **upgrade to 7.07 or 7.22 immediately**. Patching the vulnerability alone is not sufficient. Organisations should verify the integrity of affected platforms through examination of logs for evidence of successful exploitation (see Detection steps above), and report any potential malicious activity to the NCSC immediately.

If you are unable to upgrade Fortinet have also released workaround instructions that can be found on their advisory at https://www.fortiguard.com/psirt/FG-IR-22-377.

[1] https://www.fortiguard.com/psirt/FG-IR-22-377

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