



Ministry of Meteorology Energy  
Information, Disaster Management,  
Environment, Communications and  
Climate Change

**TLP: Clear<sup>1</sup>**

## **A critical vulnerability in Fortinet Fortigate SSL-VPN devices.**

Dear Constituents,

CERT Tonga is aware of a critical vulnerability which is a Remote Code Execution (CVE-2023-27997) has been identified in multiple versions of Fortinet Fortigate devices when SSL-VPN enabled.

### **How it works**

Exploitation of this vulnerability could allow a malicious actor to gain remote code execution rights on the affected system and perform unauthorised actions.

### **What to do**

To System Administrators and users, due to the critical nature of this vulnerability, we highly recommend that you upgrade your FortiOS firmware to the latest version.

- 6.0.17
- 6.2.15
- 6.4.13
- 7.0.12
- 7.2.5

### **Reference**

For further details you can also find it in the link provided.

- <https://www.fortiguard.com/psirt>

For more information, please contact us:

CERT Tonga  
Ministry of MEIDECC  
Nuku'alofa  
Tel: 2378 (CERT)  
Email: [cert@cert.gov.to](mailto:cert@cert.gov.to)  
Web: [www.cert.gov.to](http://www.cert.gov.to)  
Twitter: @CERTTonga | Facebook: @CERTTonga

1 CERT Tonga adopts the [Traffic Light Protocol](#)

**Disclaimer Notice:**

The information in this notice is intended solely for public knowledge and awareness, and not intending to harm, fright or disturb any person(s), legal entity or the receiver of this information. Under no circumstances shall the Ministry of MEIDECC be liable for any indirect, incidental, consequential, special or exemplary damages arising out of or in connection with your access or use of or inability to access or use the information and any third party content and services