GOVERNMENT OF THE REPUBLIC OF VANUATU

PRIME MINISTER'S OFFICE

CERTVU
DEPARTMENT OF COMMUNICATIONS & DIGITAL TRANSFORMATION

PM B 9108 Port Vila, Vanuatu
Tel: (678) 33380

GOUVERNEMENT DE LA REPUBLIQUE DU VANUATU

BUREAU DU PREMIER MINISTRE

CERTVU

DEPARTMENT DE COMMUNICATION ET DE TRANSFORMATION NUMERIQUE

SPP 9108 Port Vila, Vanuatu
Tel: (678) 33380

16 December 2025

Advisory 115: Fortinet Vulnerability_CVE-2025-59718 -CVE-2025-59719

Release Date: 9th of December 2025
Impact: HIGH / CRITICAL
TLP: CLEAR

The Department of Communication and Digital Transformation (DCDT through CERT Vanuatu (CERTVU), provides the following advisory.

This alert is relevant to Organizations and System/Network administrators that utilize the above products. This alert is intended to be understood by technical users and systems administrators.

What is it?

- **CVE-2025-59718:** This vulnerability involves improper verification of cryptographic signatures in versions of Fortinet FortiOS, FortiProxy, and FortiSwitchManager, which could allow an unauthenticated attacker to bypass FortiCloud SSO login authentication via a crafted SAML response message.

- **CVE-2025-59719:** This vulnerability involves improper verification of cryptographic signatures in Fortinet FortiWeb, which could allow an unauthenticated attacker to bypass FortiCloud SSO login authentication via a crafted SAML response message.

What are the Systems affected?

Affected Versions

FortiOS: 7.0.0–7.0.17, 7.2.0–7.2.11, 7.4.0–7.4.8, 7.6.0–7.6.3

FortiProxy: 7.0.0–7.0.21, 7.2.0–7.2.14, 7.4.0–7.4.10, 7.6.0–7.6.3

FortiSwitchManager: 7.0.0–7.0.5, 7.2.0–7.2.6

FortiWeb: 7.4.0–7.4.9, 7.6.0–7.6.4, 8.0.0

What does this mean?

How attackers exploit this vulnerability (attack vector)

- Full administrative compromise of Fortinet devices
- Configuration changes, creation of new admin accounts, or disabling of security controls
- Lateral movement deeper into the corporate network

Mitigation process

CERTVU recommend:

- Apply Fortinet's latest patches immediately for all affected products.
- Disable FortiCloud SSO login on devices until patched.
- Audit devices for signs of unauthorized access, new accounts, or unexpected configuration changes.
- Restrict management interface exposure to trusted IPs or VPN-only access.
- Consult the Fortinet Product Security Advisory for detailed update and mitigation information.

Reference

1. https://www.cyber.gov.au/about-us/view-all-content/alerts-and-advisories/critical-vulnerabilities-in-multiple-fortinet-products-forticloud-sso-login-authentication-bypass
2. https://fortiguard.fortinet.com/psirt/FG-IR-25-647
3. https://arcticwolf.com/resources/blog/cve-2025-59718-and-cve-2025-59719/
4. https://thehackernews.com/2025/12/fortinet-ivanti-and-sap-issue-urgent.html