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

17 July 2026

Advisory 169: Fortinet FortiSandbox OS Command Injection Vulnerability

Release Date: 16th July 2026
Impact: HIGH / CRITICAL
TLP: CLEAR

The Department of Communications 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-2026-39808 is an improper neutralization of special elements used in an OS command (OS command injection) vulnerability in Fortinet FortiSandbox 4.4.0 through 4.4.8 that may allow an attacker to execute unauthorized code or commands via a specially crafted HTTP request.

FortiSandbox is Fortinet's security solution for detecting and analysing advanced threats. It does so by detonating suspicious files and URLs in an isolated environment and returning verdicts. Other Fortinet products — firewalls, email security appliances, endpoint security clients, SIEMs, SOARs — depend on those verdicts to enforce blocking decisions or to trigger alerts and automated playbooks. FortiSandbox connects with those solutions through the Fortinet Security Fabric.

What are the systems affected?

Only FortiSandbox 4.4.0 through 4.4.8 are affected. Users should upgrade to 4.4.9 or above.

Fortinet FortiSandbox	4.40 – 4.4.8
FortiSandbox PaaS	4.4.0 – 4.4.8
FortiSandbox 5.x	Not affected by CVE-2026-39813
FortiSandbox Cloud	Partially affected

What does this mean?

The vulnerability is exploitable remotely with no authentication, no prior access, and no user interaction required.

Step 1 - Reconnaissance
The attacker identifies internet-facing FortiSandbox appliances running versions 4.4.0 through 4.4.8 via internet scanning tools such as Shodan or Censys. FortiSandbox management and API interfaces are sometimes exposed for remote administration or Fortinet Security Fabric integration.

Step 2 - Crafted HTTP Request
Both vulnerabilities can be triggered with a specially crafted HTTP request, putting unpatched FortiSandbox deployments at risk. The attacker sends a crafted HTTP request to the vulnerable unspecified API endpoint in FortiSandbox, embedding OS command injection payloads within input parameters.

Step 3 - Shell Metacharacter Injection
The application passes unsanitised metacharacters - `;`, `|`, `` ` ``, `$()` - directly into OS command construction, allowing the attacker to append arbitrary commands to the legitimate operation.

Step 4 - Unauthenticated Code Execution
Remote attackers can achieve full system compromise on affected FortiSandbox appliances, potentially leading to complete loss of confidentiality, integrity, and availability of the sandbox environment.

Step 5 - Security Fabric Poisoning
Once the FortiSandbox is compromised, the attacker can manipulate threat verdicts returned to all dependent Fortinet products - causing firewalls, email gateways, and endpoint agents to mark malicious files as safe, effectively neutralizing the entire Fortinet security stack across the organization.

Mitigation process

CERTVU recommends the following:

Upgrade to FortiSandbox 4.4.9 or Above
Obtain the update from the Fortinet Support Portal and Fortinet PSIRT advisory;

Fortinet PSIRT: https://fortiguard.fortinet.com/psirt/FG-IR-26-100
Support Portal: https://support.fortinet.com

Reference

1. https://www.cisa.gov/known-exploited-vulnerabilities-catalog
2. https://www.cve.org/CVERecord?id=CVE-2026-39808
3. https://fortiguard.fortinet.com/psirt/FG-IR-26-100
4. https://support.fortinet.com

.