CYBER ADVISORY

Wednesday, July 29, 2026 **CAL-CSIC-202607-A-014**

Two Critical Vulnerabilities found within Fortinet FortiSandbox

Arbitrary Code Execution	CIA Impacts	Crafted HTTP Requests	Patch Available

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of two critical vulnerabilities within Fortinet FortiSandbox. Fortinet FortiSandbox is an advanced threat detection and analysis solution designed to identify and mitigate zero-day malware, ransomware, and targeted cyberattacks.[1] CVE-2026-25089 carries a CVSS 3.1 score of 9.1.[2] CVE-2026-39808 carries a CVSS 3.1 score of 9.1.[3]

CVE-2026-25089 is an OS Command Injection vulnerability found within FortiSandbox, FortiSandbox Cloud, and FortiSandbox PaaS. It allows an unauthenticated attacker to execute arbitrary operating system commands on the FortiSandbox system. The flaw originates from improper neutralization of special elements used in an operating system command. Successful exploitation would allow an attacker to trigger the injection and gain full control of the underlying host to compromise its confidentiality, integrity, and availability via specially crafted HTTP requests.[4]

CVE-2026-39808 is also an OS Command Injection through API endpoint vulnerability found within FortiSandbox. The flaw originates when the sandbox service accepts unvalidated parameters that are passed directly to the operating system to allow an attacker to execute arbitrary code on the targeted host. Successful exploitation would compromise the sandbox and potentially lead to loss of confidentiality, integrity, and availability and allow an unauthenticated attacker to execute unauthenticated code or commands via crafted HTTP requests.[5]

Fortinet has acknowledged the vulnerabilities and has issued security advisories for both vulnerabilities. The Cal-CSIC recommends following the Fortinet's update guidance as soon as possible.

For additional details regarding CVE-2026-25089 and CVE-2026-39808, please use these links:

CVE-2026-25089 Security Advisory: https://fortiguard.fortinet.com/psirt/FG-IR-26-141

CVE-2026-39808 Security Advisory: https://fortiguard.fortinet.com/psirt/FG-IR-26-100

Affected Products and Versions

Vulnerability	Product	Affected Version
CVE-2026-25089	FortiSandbox 5.0	5.0.0 through 5.0.5
	FortiSandbox 4.4	4.4.0 through 4.4.8
	FortiSandbox Cloud 5.0	5.0.4 through 5.0.5
	FortiSandbox PaaS 5.0	5.0.4 through 5.0.5
CVE-2026-39808	FortiSandbox	4.4.0 through 4.4.8

Cal-CSIC services are provided at no cost to assist organizations in strengthening their cybersecurity defenses. If you need assistance or wish to verify this communication, please contact us at (833) REPORT-1, or (916) 636-2997. Visit our website for more details: California Cybersecurity Integration Center | California Governor's Office of Emergency Services

References

[1] Qualys; “Fortinet FortiSandbox Vulnerability Exploited by Attackers (CVE-2026-39808, CVE-2026-25089, & CVE-2026-39813) https://threatprotect.qualys.com/2026/06/17/fortinet-fortisandbox-vulnerability-exploited-by-attackers-cve-2026-39808-cve-2026-25089-cve-2026-39813/; accessed 29 July 2026
[2] OpenCVE; “CVE-2026-25089”; https://app.opencve.io/cve/CVE-2026-25089; accessed 29 July 2026
[3] OpenCVE; “CVE-2026-39808”; https://app.opencve.io/cve/CVE-2026-39808; accessed 29 July 2026
[4] FortiGuard Labs; “Second-Order OS Command Injection via JSON Input on start vnc feature; https://fortiguard.fortinet.com/psirt/FG-IR-26-141; accessed 29 July 2026
[5] FortiGuard Labs; “OS Command Injection through API endpoint”; https://fortiguard.fortinet.com/psirt/FG-IR-26-100; accessed 29 July 2026