CYBER ADVISORY

Friday, November 21, 2025 **CAL-CSIC- 202511-A-009**

Cyber Advisory FortiGuard Multiple Vulnerabilities

FortiGuard Products	SQL Injection	Arbitrary Code Execution	PSIRT

The California Cybersecurity Integration Center (Cal-CSIC) has identified multiple vulnerabilities affecting Fortinet products. Three of the vulnerabilities are rated as high severity, posing an immediate risk of arbitrary code execution (ACE) or privilege escalation. The most critical is CVE-2025-58692[1], a structure query language (SQL) Injection flaw (CWE-89) in the FortiVoice administrative interface with a CVSS v3.1 score of 7.7 and can be used by an authenticated attacker to execute unauthorized code or commands.

Additionally, two related vulnerabilities, CVE-2025-46373 with a CVSS v3.1 score of 7.1[2] and CVE-2025-47761 also with a CVSS v3.1 score of 7.1[3], affect FortiClient Windows. These stem from dangerous exposures in the proprietary FortIPS kernel driver that can lead to Arbitrary Code Execution/Arbitrary Memory Write, enabling an authenticated local user to execute unauthorized code and potentially escalate privileges.

The Cal-CSIC recommends immediately applying the patches corresponding to the vulnerabilities listed in the table below, with priority given to the High-severity issues affecting FortiVoice and FortiClient Windows.

For further information on applying these patches, please refer to PSIRT Advisories | FortiGuard Labs[4]

Table of Fortiguard CVEs:

CVE ID	CVSS Score	Severity	Description	Affected Product & Version(s)	Solution
CVE-2025-58692	7.7	High	**SQL Injection** (CWE-89) in FortiVoice administrative interface, allowing an authenticated attacker to execute unauthorized code/commands.	**FortiVoice** 7.2.0-7.2.2, 7.0.0-7.0.7.	**Upgrade** 7.2 to 7.2.3+ or 7.0 to 7.0.8+.
CVE-2025-46373	7.1	High	**Buffer Overflow via fortips Driver** (CWE-122) in FortiClient Windows, allowing an authenticated local IPSec user to execute arbitrary code/commands.	**FortiClientWindows** 7.4.0-7.4.3, 7.2.0-7.2.8.	**Upgrade** 7.4 to 7.4.4+ or 7.2 to 7.2.9+.
CVE-2025-47761	7.1	High	**Arbitrary Memory Write via FortIPS Driver** (CWE-782) in FortiClient Windows, allowing an authenticated local user to execute unauthorized code via the driver.	**FortiClientWindows** 7.4.0-7.4.3, 7.2.0-7.2.9.	**Upgrade** 7.4 to 7.4.4+ or 7.2 to 7.2.10+.
No Assigned CVE ID (FG-IR-25-545)	N/A	Low	**Trusted Hosts Bypass via SSH** (CWE-269) in FortiOS, FortiProxy, and FortiPAM allowing an authenticated admin to bypass the trusted host policy via crafted CLI command.	**FortiOS** 7.6.0-7.6.3, all versions of 7.4/7.2/7.0/6.4. **FortiPAM** 1.6.0, all versions of 1.5/1.4/1.3/1.2/1.1/1.0. **FortiProxy** 7.6.0-7.6.3, all versions of 7.4/7.2/7.0.	**Upgrade** FortiOS/FortiProxy 7.6 to 7.6.4+. **Upgrade** FortiPAM 1.6 to 1.6.1+. **Migrate** other affected versions to a fixed release.
CVE-2025-54971	3.9	Low	**Information Disclosure through Debug Features** (CWE-200) in FortiADC Logs, allowing a read-only admin to obtain external resources passwords.	**FortiADC** 7.4.0, all versions of 7.2, 7.1, 7.0, and 6.2.	**Upgrade** 7.4 to 7.4.3+. **Migrate** other versions to a fixed release. **Workaround**: Disable external resources via CLI.
CVE-2025-61713	3.8	Low	**Cleartext Credentials in Diagnose Output** (CWE-316) in FortiPAM, allowing an authenticated attacker with read-write admin privileges to obtain other administrators' credentials.	**FortiPAM** 1.6.0, all versions of 1.5, 1.4, 1.3, 1.2, 1.1, and 1.0.	**Upgrade** 1.6 to 1.6.1+. **Migrate** other versions to a fixed release.
CVE-2025-54972	3.9	Low	**CRLF Header Injection in Webmail User GUI** (CWE-93) in FortiMail, allowing an attacker to inject headers by convincing a user to click a crafted link.	**FortiMail** 7.6.0-7.6.3, 7.4.0-7.4.5, all versions of 7.2 and 7.0.	**Upgrade** 7.6 to 7.6.4+ or 7.4 to upcoming 7.4.6+. **Migrate** 7.2/7.0 to a fixed release.
CVE-2025-58034	6.7	Medium	**Multiple OS Command Injection in API and CLI** in FortiWeb via crafted HTTP requests or CLI commands.	**FortiWeb** 8.0.0-8.0.1, 7.6.0-7.6.5, 7.4.0-7.4.10, 7.2.0-7.2.11, 7.0.0-7.0.11	**Upgrade** to 8.0.2+, 7.6.6+, 7.4.11+, 7.2.12+, or 7.0.12+.

CVE-2025-58412	4.2	Medium	**XSS in Default Error Page** (CWE-80) in FortiADC virtual server's default error page via crafted URL.	**FortiADC** 8.0.0, 7.6.0-7.6.3, all versions of 7.4 and 7.2.	**Upgrade** to 8.0.1+ or 7.6.4+. **Migrate** 7.4/7.2 to a fixed release. **Workaround**: Customize waf_deny.html error page.
CVE-2025-59669	4.8	Medium	**Use of Hardcoded Password for Redis Service** (CWE-798) in FortiWeb internal redis services, allowing an authenticated attacker with shell access to access its data.	**FortiWeb** 7.6.0, all versions of 7.4, 7.2, and 7.0.	**Upgrade** 7.6 to 7.6.1+. **Migrate** 7.4, 7.2, 7.0 to a fixed release.
CVE-2025-53843	6.9	Medium	**Stack Buffer Overflow in CAPWAP Daemon** (CWE-124) in FortiOS and FortiSwitchManager, allowing a remote authenticated attacker to execute arbitrary code.	**FortiOS** 7.6.0-7.6.3, 7.4.0-7.4.8, all versions of 7.2, 7.0, and 6.4.	**Upgrade** 7.6 to 7.6.4+ or 7.4 to 7.4.9+. **Migrate** 7.2, 7.0, 6.4 to a fixed release.
CVE-2025-58413	6.9	Medium	**Stack Buffer Overflow in CAPWAP Daemon** (CWE-124) in FortiOS allowing a remote **unauthenticated** attacker on an adjacent network to achieve arbitrary code execution.	**FortiOS** 7.6.0-7.6.3, 7.4.0-7.4.8, all versions of 7.2/7.0/6.4/6.2/6.0. **FortiSASE** 25.3.b.	**Upgrade** FortiOS 7.6 to 7.6.4+ or 7.4 to 7.4.9+. **Migrate** other FortiOS versions to a fixed release. **FortiSASE 25.3.b** is remediated in 25.3.c.
CVE-2025-48839	6.3	Medium	**Out-of-bounds Write** (CWE-787) in FortiADC, allowing an authenticated attacker to execute arbitrary code via crafted HTTP requests.	**FortiADC** 8.0.0, 7.6.0-7.6.2, 7.4.0-7.4.7, all versions of 7.2/7.1/7.0/6.2.	**Upgrade** 8.0 to 8.0.1+, 7.6 to 7.6.3+, or 7.4 to 7.4.8+. **Migrate** older versions to a fixed release.
CVE-2025-54660	4.9	Medium	**Information Disclosure through Debug Features** (CWE-489) in FortiClientWindows, allowing a local attacker to retrieve the saved VPN user password.	**FortiClientWindows** 7.4.0-7.4.3, 7.2.0-7.2.10, all versions of 7.0.	**Upgrade** 7.4 to 7.4.4+ or 7.2 to 7.2.11+. **Migrate** 7.0 to a fixed release.
CVE-2025-46215	5	Medium	**File Scan Result Bypass** (CWE-653) in FortiSandbox, allowing an unauthenticated attacker to evade the sandboxing scan via a crafted file.	**FortiSandbox** 5.0.0-5.0.1, 4.4.0-4.4.7, all versions of 4.2 and 4.0.	**Upgrade** 5.0 to 5.0.2+ or 4.4 to 4.4.8+. **Migrate** 4.2/4.0 to a fixed release. **Workaround for 4.4**: Upgrade Tracer Engine to 04004.00477+.
CVE-2025-46775	5.2	Medium	**Credential Leakage through Debug Commands** (CWE-522) in FortiExtender, allowing an authenticated user to obtain administrator credentials via debug log commands.	**FortiExtender** 7.6.0-7.6.1, 7.4.0-7.4.6, all versions of 7.2 and 7.0.	**Upgrade** 7.6 to 7.6.3+ or 7.4 to 7.4.8+. **Migrate** 7.2/7.0 to a fixed release.

CVE-2025-46776	6.3	Medium	**Authenticated CLI Commands Buffer Overflow** (CWE-120) in FortiExtender json_cli, allowing an authenticated user to execute arbitrary code or commands.	**FortiExtender** 7.6.0-7.6.1, 7.4.0-7.4.6, all versions of 7.2 and 7.0.	**Upgrade** 7.6 to 7.6.3+ or 7.4 to 7.4.8+. **Migrate** 7.2/7.0 to a fixed release.

References:

[1] FortiGuard Labs; "Vulnerability Report: FortiAnalyzer Out-of-bounds Read (CVE-2025-58692)" https://www.fortiguard.com/advisory/CVE-2025-58692; accessed 21 November 2025
[2] FortiGuard Labs; "Advisory: FortiOS and FortiProxy Multiple Vulnerabilities (CVE-2025-46373)" https://www.fortiguard.com/advisory/CVE-2025-46373; accessed 21 November 2025
[3] FortiGuard Labs; "Security Notice: FortiManager Remote Code Execution (CVE-2025-47761)" https://www.fortiguard.com/advisory/CVE-2025-47761; accessed 21 November 2025
[4] FortiGuard Labs; "PSIRT Advisories" https://fortiguard.fortinet.com/psirt; accessed 19 November 2025