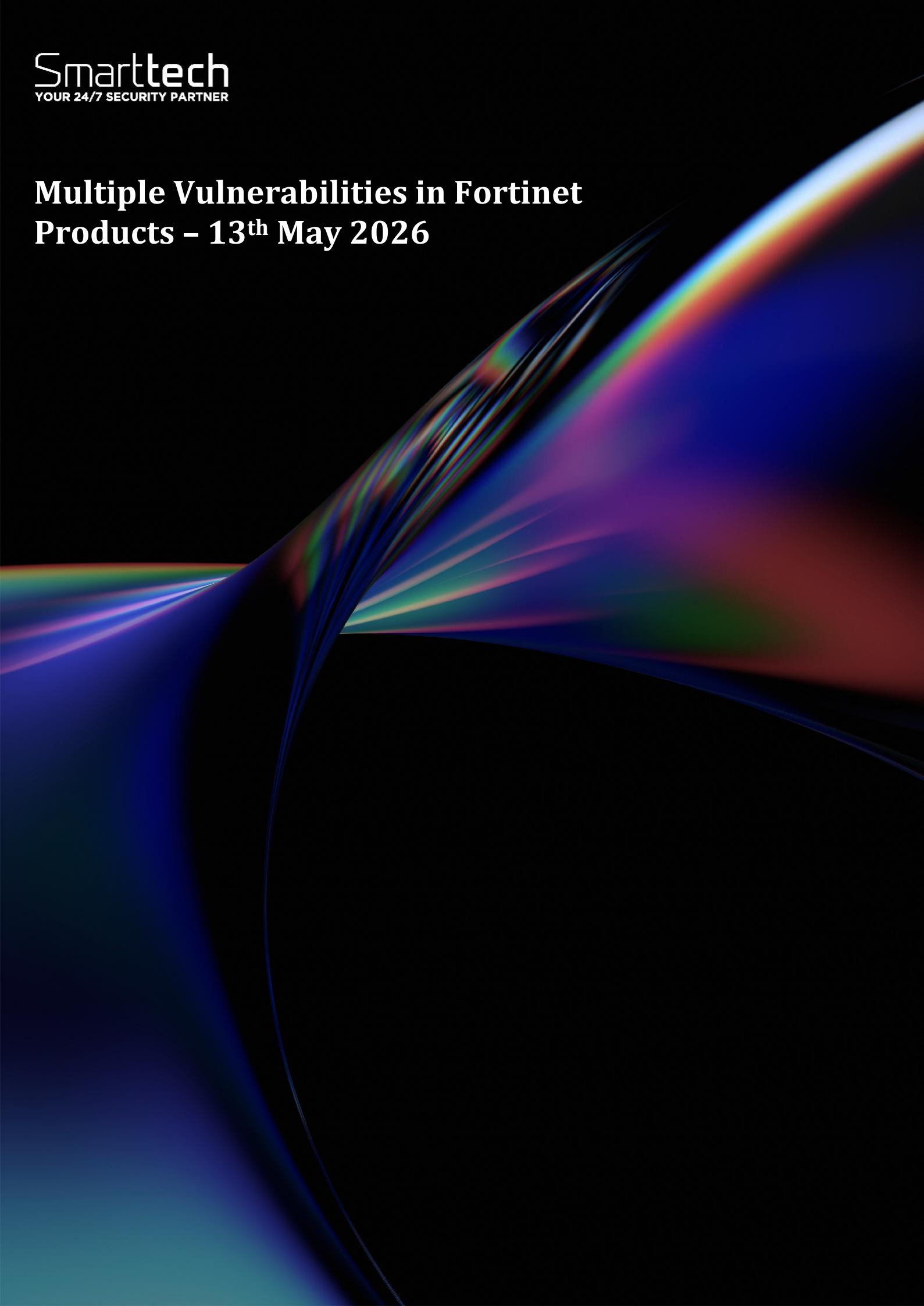
Smarttech
YOUR 24/7 SECURITY PARTNER

Multiple Vulnerabilities in Fortinet Products – 13th May 2026



Document ID	SMA-Threat Report
Document status	ISSUED
Issue Number	70
Authors	Maria-Iasmina Macovei < maria.macovei@smarttech247.com >
Verified by	Alin Curcan < alin.curcan@smarttech247.com >
Last modified	2026-05-13
Issue Date	2026-05-12

Threat Reports are reports created by Smarttech247 based on high and critical severity vulnerabilities that may have a high potential to be exploited in the wild i.e. vulnerabilities that are present in most used products by companies and do not have an auto-update option or they are usually not automatically updated in case that could lead to some service disruption. This report is usually created as soon as the vulnerability is released, therefore we strongly recommend that the information is reviewed, tests are performed and patches are applied before the first proof-of-concept is released. Even though certain vulnerabilities may not have an active exploit in the wild at the time that we report on them, we take into consideration the wider risk and the impact it could have on systems, should an exploit like that be available after a while. Our duty is to report them on time and we recommend enterprises that, in order to keep critical business systems protected, they should consider, on average, ten working days to check whether or not the new vulnerability affects them, and if so, to implement actions in order to remove the risk.

Overview:

Multiple vulnerabilities were discovered across several Fortinet products, the most severe of which could allow attackers to execute arbitrary code, escalate privileges, bypass authentication or security restrictions, access sensitive information, or cause denial-of-service conditions. Depending on the privileges of the affected service or user, successful exploitation could enable an attacker to modify or delete data, alter security configurations, create administrative accounts, or otherwise gain full control of the impacted system, leading to complete compromise.

Risk

Government:

- Large and medium government entities: High
- Small government entities: Medium

Businesses:

- Large and medium business entities: High
- Small business entities: Medium

Technical summary

CVE ID	*Description*	*Version*	*Affected*	*Solution*
CVE-2025-53844 (CVSS Score 8.3)	An Out-Of-Bounds Write vulnerability [CWE-787] in FortiOS capwap daemon may allow an attacker controlling an authenticated FortiAP FortiExtender or FortiSwitch to gain execution privileges on the FortiGate device.	FortiOS 7.6	7.6.0 through 7.6.3	Upgrade to 7.6.4 or above
		FortiOS 7.4	7.4.0 through 7.4.8	Upgrade to 7.4.9 or above
		FortiOS 7.2	7.2.0 through 7.2.11	Upgrade to 7.2.12 or above
CVE-2025-53870 (CVSS Score 6.5)	An OS command injection vulnerabtility [CWE-78] in FortiAP and FortiAP-W2 cli may allow an authenticated attacker to execute unauthorized code or commands via a specifically crafted cli command.	FortiAP 7.6	7.6.0 through 7.6.2	Upgrade to 7.6.3 or above
		FortiAP 7.4	7.4.0 through 7.4.5	Upgrade to 7.4.6 or above
		FortiAP 7.2	7.2 all versions	Migrate to a fixed release
		FortiAP 6.4	6.4 all versions	Migrate to a fixed release
		FortiAP-W2 7.4	7.4.0 through 7.4.4	Upgrade to 7.4.5 or above
		FortiAP-W2 7.2	7.2.0 through 7.2.5	Upgrade to upcoming 7.2.6

				or above
CVE-2026-26083 (CVSS Score 9.1)	A missing authorization vulnerability [CWE-862] in FortiSandbox, FortiSandbox Cloud and FortiSandbox PaaS WEB UI may allow an unauthenticated attacker to execute unauthorized code or commands via HTTP requests.	FortiSandbox 5.0	5.0.0 through 5.0.1	Upgrade to 5.0.2 or above
		FortiSandbox 4.4	4.4.0 through 4.4.8	Upgrade to 4.4.9 or above
		FortiSandbox Cloud 24	All versions	Migrate to a fixed release
		FortiSandbox Cloud 23	All versions	Migrate to a fixed release
		FortiSandbox Cloud 5.0	5.0.2 through 5.0.5	Upgrade to 5.0.6 or above
		FortiSandbox PaaS 23.4	23.4 all versions	Migrate to a fixed release
		FortiSandbox PaaS 23.3	23.3 all versions	Migrate to a fixed release
		FortiSandbox PaaS 23.1	23.1 all versions	Migrate to a fixed release
		FortiSandbox PaaS 22.2	22.2 all versions	Migrate to a fixed release
		FortiSandbox PaaS 22.1	22.1 all versions	Migrate to a fixed release
		FortiSandbox PaaS 21.4	21.4 all versions	Migrate to a fixed release
		FortiSandbox PaaS 21.3	21.3 all versions	Migrate to a fixed release
		FortiSandbox PaaS 5.0	5.0.0 through 5.0.1	Upgrade to 5.0.2 or above
		FortiSandbox PaaS 4.4	4.4.5 through 4.4.8	Upgrade to 4.4.9 or above
CVE-2025-67604 (CVSS Score 5.2)	A use of potentially Dangerous Function vulnerability [CWE-676] in FortiAnalyzer and FortiManager API may allow an authenticated attacker to cause a system hang via multiple specially crafted HTTP requests causing crashes. This happens if internal locks are aligned, which is out of control of the attacker.	FortiAnalyzer 8.0	Not affected	Not Applicable
		FortiAnalyzer 7.6	7.6.0 through 7.6.4	Upgrade to 7.6.5 or above
		FortiAnalyzer 7.4	7.4.0 through 7.4.8	Upgrade to 7.4.9 or above
		FortiAnalyzer 7.2	7.2 all versions	Migrate to a fixed release
		FortiManager 8.0	Not affected	Not Applicable
		FortiManager 7.6	7.6.0 through 7.6.4	Upgrade to 7.6.5 or above
		FortiManager 7.4	7.4.0 through 7.4.8	Upgrade to 7.4.9 or above
		FortiManager 7.2	7.2 all versions	Migrate to a fixed release
CVE-2025-53680 (CVSS Score 6.1)	An improper neutralization of special elements used in an OS command ("OS Command Injection") vulnerability [CWE-78] in FortiAP, FortiAP-U & FortiAP-W2 CLI may allow an authenticated privileged attacker to execute unauthorized code or commands via crafted CLI requests.	FortiAP 7.6	7.6.0 through 7.6.2	Upgrade to 7.6.3 or above
		FortiAP 7.4	7.4.0 through 7.4.5	Upgrade to 7.4.6 or above
		FortiAP 7.2	7.2 all versions	Migrate to a fixed release
		FortiAP 6.4	6.4 all versions	Migrate to a fixed release
		FortiAP-U 7.0	7.0.0 through 7.0.5	Upgrade to 7.0.6 or above

		FortiAP-W2 7.4	7.4.0 through 7.4.4	Upgrade to 7.4.5 or above
		FortiAP-W2 7.2	7.2 all versions	Migrate to a fixed release

Recommendations

Smarttech247 team recommend the following actions be taken:

- Apply the stable channel update provided by Fortinet to vulnerable systems immediately after appropriate testing. (**M1051**: **Update Software**)
    - **Safeguard 7.1: Establish and Maintain a Vulnerability Management Process**: Establish and maintain a documented vulnerability management process for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.
    - **Safeguard 7.2: Establish and Maintain a Remediation Process**: Establish and maintain a risk-based remediation strategy documented in a remediation process, with monthly, or more frequent, reviews.
    - **Safeguard 7.4: Perform Automated Application Patch Management**: Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.
    - **Safeguard 7.6: Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets**: Perform automated vulnerability scans of externally-exposed enterprise assets using a SCAP-compliant vulnerability scanning tool. Perform scans on a monthly, or more frequent, basis.
    - **Safeguard 7.7: Remediate Detected Vulnerabilities**: Remediate detected vulnerabilities in software through processes and tooling on a monthly, or more frequent, basis, based on the remediation process.
    - **Safeguard 16.13 Conduct Application Penetration Testing**: Conduct application penetration testing. For critical applications, authenticated penetration testing is better suited to finding business logic vulnerabilities than code scanning and automated security testing. Penetration testing relies on the skill of the tester to manually manipulate an application as an authenticated and unauthenticated user.
    - **Safeguard 12.1: Ensure Network Infrastructure is Up-to-Date**: Ensure network infrastructure is kept up-to-date. Example implementations include running the latest stable release of software and/or using currently supported network-as-a-service (NaaS) offerings. Review software versions monthly, or more frequently, to verify software support.
    - **Safeguard 18.1: Establish and Maintain a Penetration Testing Program**: Establish and maintain a penetration testing program appropriate to the size, complexity, and maturity of the enterprise. Penetration testing program characteristics include scope, such as network, web application, Application Programming Interface (API), hosted services, and physical premise controls; frequency; limitations, such as acceptable hours, and excluded attack types; point of contact information; remediation, such as how findings will be routed internally; and retrospective requirements.
    - **Safeguard 18.2: Perform Periodic External Penetration Tests**: Perform periodic external penetration tests based on program requirements, no less than annually. External penetration testing must include enterprise and environmental reconnaissance to detect exploitable information. Penetration testing requires specialized skills and experience and must be conducted through a qualified party. The testing may be clear box or opaque box.

    - **Safeguard 18.3: Remediate Penetration Test Findings**: Remediate penetration test findings based on the enterprise's policy for remediation scope and prioritization.

- Apply the Principle of Least Privilege to all systems and services. Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack. (**M1026**: Privileged Account Management)
    - **Safeguard 4.7: Manage Default Accounts on Enterprise Assets and Software**: Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.
    - **Safeguard 5.4: Restrict Administrator Privileges to Dedicated Administrator Accounts**: Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.

- Vulnerability scanning is used to find potentially exploitable software vulnerabilities to remediate them. (**M1016**: Vulnerability Scanning)
    - **Safeguard 16.13: Conduct Application Penetration Testing**: Conduct application penetration testing. For critical applications, authenticated penetration testing is better suited to finding business logic vulnerabilities than code scanning and automated security testing. Penetration testing relies on the skill of the tester to manually manipulate an application as an authenticated and unauthenticated user.

- Architect sections of the network to isolate critical systems, functions, or resources. Use physical and logical segmentation to prevent access to potentially sensitive systems and information. Use a DMZ to contain any internet-facing services that should not be exposed from the internal network. Configure separate virtual private cloud (VPC) instances to isolate critical cloud systems. (**M1030**: Network Segmentation)
    - **Safeguard 12.2: Establish and Maintain a Secure Network Architecture**: Establish and maintain a secure network architecture. A secure network architecture must address segmentation, least privilege, and availability, at a minimum.

- Use capabilities to detect and block conditions that may lead to or be indicative of a software exploit occurring. (**M1050**: Exploit Protection)
    - **Safeguard 10.5: Enable Anti-Exploitation Features**: Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.

References

https://www.fortiguard.com/psirt/FG-IR-26-123
https://www.fortiguard.com/psirt/FG-IR-26-133
https://www.fortiguard.com/psirt/FG-IR-26-136
https://www.fortiguard.com/psirt/FG-IR-26-137
https://www.fortiguard.com/psirt/FG-IR-26-131

CVEs

CVE-2025-53844
CVE-2025-53870
CVE-2026-26083
CVE-2025-67604
CVE-2025-53680

Smarttech
YOUR 24/7 SECURITY PARTNER

www.smarttech247.com