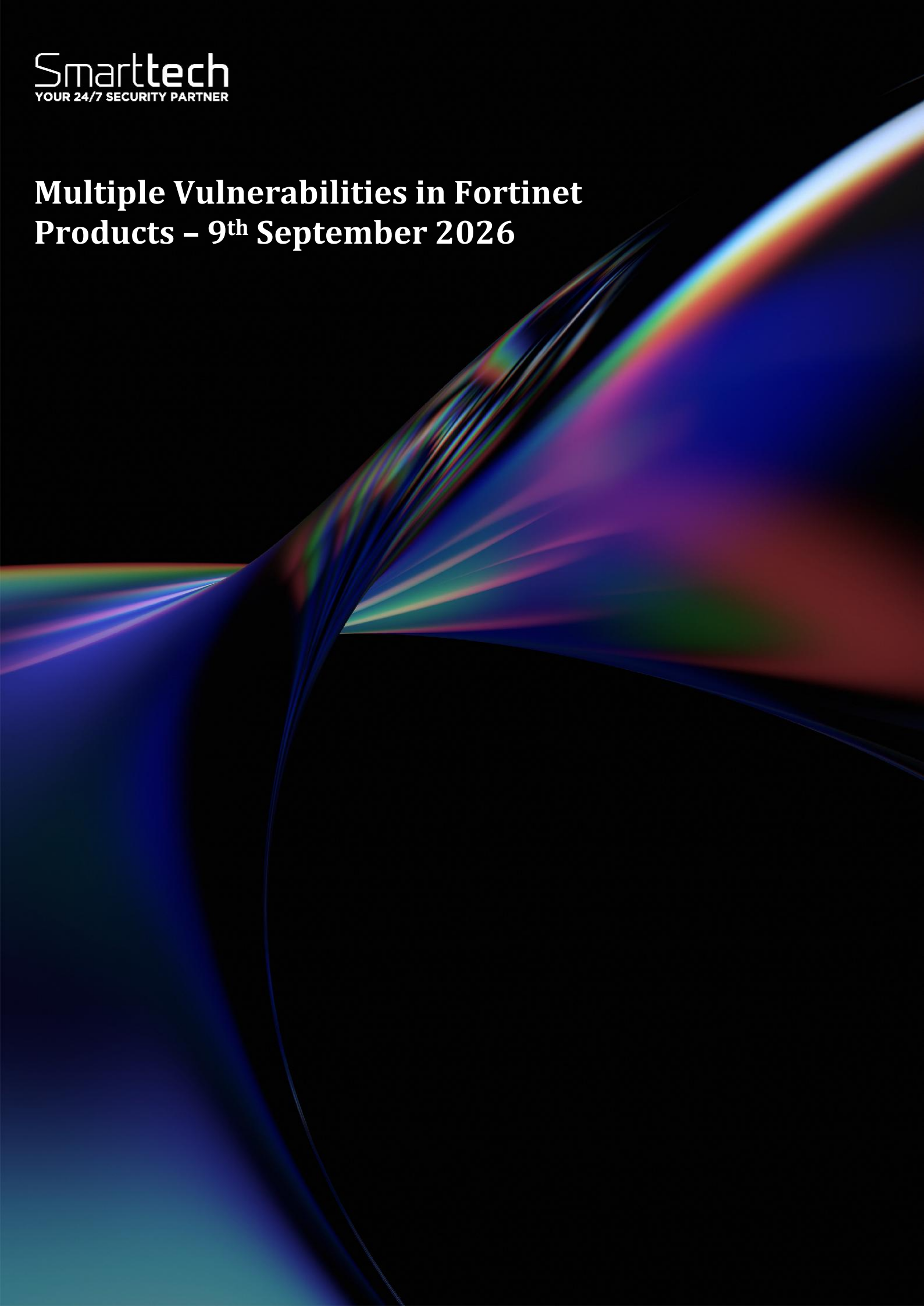


Multiple Vulnerabilities in Fortinet Products – 9th September 2026



Document ID	SMA-Threat Report
Document status	ISSUED
Issue Number	158
Authors	Dorin Constantin Banu < constantin.banu@smarttech247.com >
Verified by	Catalin Nita < catalin.nita@smarttech247.com >
Last modified	2026-09-09
Issue Date	2026-09-09

This document and any information therein are confidential property of Smarttech247 and without infringement neither the whole nor any extract may be disclosed, loaned, copied or used for manufacturing, provision of services or other purposes whatsoever without prior written consent of Smarttech247, and no liability is accepted for loss or damage from any cause whatsoever from the use of the document. Smarttech247 retain the right to alter the document at any time unless a written statement to the contrary has been appended.

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 identified across several Fortinet products, which could allow attackers to access sensitive information, execute unauthorized code or commands, bypass security controls, perform Man-in-the-Middle attacks, or cause denial-of-service conditions. Depending on the affected product and deployment, successful exploitation could lead to information disclosure, unauthorized code or command execution, security control bypass, Man-in-the-Middle attacks, or service disruption.

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-2026-84387 (CVSS Score 6.7)	An Improper Neutralization of Special Elements used in a Command ('Command Injection') vulnerability [CWE-77] in FortiSandbox may allow a privileged attacker to execute unauthorized code or commands via crafted HTTP requests.	FortiSandbox 5.2	5.2.0	Upgrade to 5.2.1 or above
		FortiSandbox 5.0	5.0.0 through 5.0.6	Upgrade to 5.0.7 or above
		FortiSandbox 4.4	4.4.0 through 4.4.9	Upgrade to 4.4.10 or above
CVE-2026-84392 (CVSS Score 2.5)	A NULL Pointer Dereference vulnerability [CWE-476] in FortiOS, FortiProxy and FortiPAM may allow an authenticated attacker to crash the httpsd daemon via crafted HTTP requests.	FortiOS 8.0	Not affected	Not Applicable
		FortiOS 7.6	Not affected	Not Applicable
		FortiOS 7.4	7.4 all versions	Migrate to a fixed release
		FortiOS 7.2	7.2 all versions	Migrate to a fixed release
		FortiPAM 1.9	1.9.0	Upgrade to 1.9.1 or above
		FortiPAM 1.8	1.8 all versions	Migrate to a fixed release

		FortiPAM 1.7	1.7 all versions	Migrate to a fixed release
		FortiPAM 1.6	1.6 all versions	Migrate to a fixed release
		FortiPAM 1.5	1.5 all versions	Migrate to a fixed release
		FortiPAM 1.4	1.4 all versions	Migrate to a fixed release
		FortiPAM 1.3	1.3 all versions	Migrate to a fixed release
		FortiPAM 1.2	1.2 all versions	Migrate to a fixed release
		FortiPAM 1.1	1.1 all versions	Migrate to a fixed release
		FortiPAM 1.0	1.0 all versions	Migrate to a fixed release
		FortiProxy 7.6	7.6.0 through 7.6.6	Upgrade to 7.6.7 or above
		FortiProxy 7.4	7.4 all versions	Migrate to a fixed release
		FortiProxy 7.2	7.2 all versions	Migrate to a fixed release
CVE-2026-26084 (CVSS Score 8.9)	An improper access control vulnerability [CWE-284] in FortiSandbox, FortiSandbox Cloud and FortiSandbox PaaS WEB UI may allow an unauthenticated attacker to access sensitive information via crafted HTTP requests.	FortiSandbox 5.2	Not affected	Not Applicable
		FortiSandbox 5.0	5.0.0 through 5.0.5	Upgrade to 5.0.6 or above
		FortiSandbox 4.4	4.4.0 through 4.4.8	Upgrade to 4.4.9 or above
		FortiSandbox Cloud 5.0	5.0.4 through 5.0.5	Upgrade to 5.0.6 or above
		FortiSandbox Cloud 4.4	Not affected	Not Applicable
		FortiSandbox PaaS 5.2	Not affected	Not Applicable
		FortiSandbox PaaS 5.0	5.0.4 through 5.0.5	Upgrade to 5.0.6 or above
CVE-2026-84391 (CVSS Score 5.9)	A Use of Uninitialized Variable [CWE-457] vulnerability in Fortinet FortiAnalyzer SNMP daemon may allow a remote authenticated attacker with user permission to cause a denial of service via SNMP GETBULK requests.	FortiAnalyzer 8.0	Not affected	Not Applicable
		FortiAnalyzer 7.6	7.6.3 through 7.6.6	Upgrade to 7.6.7 or above
		FortiAnalyzer 7.4	Not affected	Not Applicable
		FortiAnalyzer 7.2	Not affected	Not Applicable
CVE-2026-22575 (CVSS Score 4.7)	An improper access control vulnerability [CWE-284] in FortiManager may allow an administrator to bypass the approval process for workflow sessions via crafted HTTP or	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	Upgrade to

	HTTPs requests.		through 7.4.10	7.4.11 or above
		FortiManager 7.2	7.2 all versions	Migrate to a fixed release
		FortiManager Cloud 7.6	7.6.2 through 7.6.4	Upgrade to 7.6.5 or above
		FortiManager Cloud 7.4	7.4.1 through 7.4.10	Upgrade to upcoming 7.4.11 or above
		FortiManager Cloud 7.2	7.2 all versions	Migrate to a fixed release
CVE-2026-84393 (CVSS Score 7.3)	An improper certificate validation vulnerability [CWE-295] in FortiOS and FortiProxy Agentless ZTNA portal may allow a remote and unauthenticated attacker to perform a Man-in-the-Middle attack on the communication channel between the ZTNA portal and the backend destination website.	FortiOS 8.0	Not affected	Not Applicable
		FortiOS 7.6	7.6.1 through 7.6.6	Upgrade to 7.6.7 or above
		FortiOS 7.4	Not affected	Not Applicable
		FortiOS 7.2	Not affected	Not Applicable
		FortiProxy 8.0	Not affected	Not Applicable
		FortiProxy 7.6	7.6.2 through 7.6.6	Upgrade to 7.6.7 or above
		FortiProxy 7.4	Not affected	Not Applicable
		FortiProxy 7.2	Not affected	Not Applicable

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-26-167>
<https://www.fortiguard.com/psirt/FG-IR-26-173>
<https://www.fortiguard.com/psirt/FG-IR-26-166>
<https://www.fortiguard.com/psirt/FG-IR-26-172>
<https://www.fortiguard.com/psirt/FG-IR-26-171>
<https://www.fortiguard.com/psirt/FG-IR-26-174>

CVEs

CVE-2026-84387
CVE-2026-84392
CVE-2026-26084
CVE-2026-84391
CVE-2026-22575
CVE-2026-84393

