Smarttech
YOUR 24/7 SECURITY PARTNER

Multiple Vulnerabilities in Fortinet Products

Document ID	SMA-Threat Report
Document status	ISSUED
Issue Number	52
Authors	Mariana Babadac < ana.nastase@smarttech247.com >
Verified by	Alin Curcan < alin.curcan@smarttech247.com >
Last modified	2026-04-15
Issue Date	2026-04-14

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 execute unauthorized code or commands, bypass authentication mechanisms, perform path traversal, access sensitive information, or modify and delete files. Some vulnerabilities may also enable attackers to retain access, manipulate configurations, or perform web-based attacks such as XSS and SQL injection.

Depending on the level of access, successful exploitation could allow attackers to impact system integrity, access or alter data, and potentially compromise affected systems.

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-2026-25691 (CVSS Score 6.2)	An Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability [CWE-22] in FortiSandbox, FortiSandbox Cloud, FortiSandbox PaaS and FortiSandbox Cloud WEB UI may allow a privileged attacker with super-admin profile and CLI access to delete an arbitrary directory via HTTP crafted 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 4.2	4.2 all versions	Migrate to a fixed release
		FortiSandbox Cloud 24	Not affected	Not Applicable
		FortiSandbox Cloud 23	Not affected	Not Applicable
		FortiSandbox Cloud 5.0	5.0.4	Fortinet remediated

				this issue in 5.0.5 and hence customers do not need to perform any action.
		FortiSandbox Cloud 4.4	Not affected	Not Applicable
		FortiSandbox Cloud 4.2	Not affected	Not Applicable
		FortiSandbox PaaS 5.0	5.0.4	Upgrade to 5.0.5 or above
		FortiSandbox PaaS 4.4	Not affected	Not Applicable
		FortiSandbox PaaS 4.2	Not affected	Not Applicable
CVE-2026-27316 (CVSS Score 2.5)	An Insufficiently protected credentials vulnerability [CWE-522] in FortiSanbox and FortiSanbox PaaS GUI may allow an authenticated administrator to read LDAP server credentials via client-side inspection.	FortiSandbox 5.0	5.0.0 through 5.0.5	Upgrade to 5.0.6 or above
		FortiSandbox 4.4	4.4 all versions	Migrate to a fixed release
		FortiSandbox PaaS 5.0	5.0.1 through 5.0.5	Upgrade to 5.0.6 or above
CVE-2026-22828 (CVSS Score 7.3)	A heap-based buffer overflow vulnerability [CWE-122] in FortiAnalyzer Cloud oftpd daemon may allow a remote unauthenticated attacker to execute arbitrary code or commands via specifically crafted requests. Successful exploitation would require a large amount of effort in preparation because of ASLR and network segmentation	FortiAnalyzer Cloud 7.6	7.6.2 through 7.6.4	Upgrade to 7.6.5 or above
		FortiManager Cloud 7.6	7.6.2 through 7.6.4	Upgrade to 7.6.5 or above
CVE-2025-53847 (CVSS Score 6.2)	A missing authentication for critical function vulnerability [CWE-306] in FortiOS and FortiSwitchManager CAPWAP daemon may allow a local unauthenticated attacker on the same local IP subnet to write device configuration via specially crafted requests. To be successful, this attack requires the targeted FortiGate device to run a specific, non default configuration.	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
		FortiOS 7.0	7.0.0 through 7.0.17	Upgrade to 7.0.18 or above
		FortiOS 6.4	6.4 all versions	Migrate to a fixed release
		FortiOS 6.2	6.2.9 through 6.2.17	Migrate to a fixed release
CVE-2026-39812 (CVSS Score	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	FortiSandbox 5.0	5.0.0 through 5.0.5	Upgrade to 5.0.6 or above

6.7)	vulnerability [CWE-79] in FortiSandbox and FortiSandbox Cloud may allow a privileged attacker to perform a stored XSS attack via crafted HTTP requests.	FortiSandbox 4.4	4.4.0 through 4.4.8	Upgrade to 4.4.9 or above
		FortiSandbox 4.2	4.2 all versions	Migrate to a fixed release
		FortiSandbox PaaS 5.0	5.0.0 through 5.0.5	Upgrade to 5.0.6 or above
		FortiSandbox PaaS 4.4	4.4.0 through 4.4.8	Upgrade to 4.4.9 or above
		FortiSandbox PaaS 4.2	4.2 all versions	Migrate to a fixed release
CVE-2026-39808 (CVSS Score 9.1)	An Improper Neutralization of Special Elements used in an OS Command ('OS command injection') vulnerability [CWE-78] in FortiSandbox may allow an unauthenticated attacker to execute unauthorized code or commands via crafted HTTP requests.	FortiSandbox 5.0	Not affected	Not Applicable
		FortiSandbox 4.4	4.4.0 through 4.4.8	Upgrade to 4.4.9 or above
CVE-2025-68649 (CVSS Score 5.4)	An improper limitation of a pathname to a restricted directory ('path traversal') vulnerability in FortiAnalyzer, FortiAnalyzer Cloud, FortiManager and FortiManager Cloud may allow a privileged attacker to delete files from the underlying filesystem via crafted CLI requests.	FortiAnalyzer 7.6	7.6.0 through 7.6.4	Upgrade to 7.6.5 or above
		FortiAnalyzer 7.4	7.4.0 through 7.4.7	Upgrade to 7.4.8 or above
		FortiAnalyzer 7.2	7.2 all versions	Migrate to a fixed release
		FortiAnalyzer 7.0	7.0 all versions	Migrate to a fixed release
		FortiAnalyzer 6.4	Not affected	Not Applicable
		FortiAnalyzer Cloud 7.6	7.6.0 through 7.6.4	Upgrade to 7.6.5 or above
		FortiAnalyzer Cloud 7.4	7.4.0 through 7.4.7	Upgrade to 7.4.8 or above
		FortiAnalyzer Cloud 7.2	7.2 all versions	Migrate to a fixed release
		FortiAnalyzer Cloud 7.0	7.0 all versions	Migrate to a fixed release
		FortiManager 7.6	7.6.0 through 7.6.4	Upgrade to 7.6.5 or above
		FortiManager 7.4	7.4.0 through 7.4.7	Upgrade to 7.4.8 or above
		FortiManager 7.2	7.2 all versions	Migrate to a fixed release
		FortiManager 7.0	7.0 all versions	Migrate to a fixed release

		FortiManager 6.4	Not affected	Not Applicable
		FortiManager Cloud 7.6	7.6.0 through 7.6.4	Upgrade to 7.6.5 or above
		FortiManager Cloud 7.4	7.4.0 through 7.4.7	Upgrade to 7.4.8 or above
		FortiManager Cloud 7.2	7.2 all versions	Migrate to a fixed release
		FortiManager Cloud 7.0	7.0 all versions	Migrate to a fixed release
CVE-2025-61624(CVSS Score 5.4) Known Exploited	An Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') [CWE-22] in the command line interpreter of FortiOS, FortiPAM, FortiProxy and FortiSwitchManager may allow a privileged attacker to achieve arbitrary write or delete files via specifically crafted arguments to existing commands.	FortiOS 7.6	7.6.0 through 7.6.4	Upgrade to 7.6.5 or above
		FortiOS 7.4	7.4.0 through 7.4.9	Upgrade to 7.4.10 or above
		FortiOS 7.2	7.2 all versions	Migrate to a fixed release
		FortiOS 7.0	7.0 all versions	Migrate to a fixed release
		FortiOS 6.4	6.4 all versions	Migrate to a fixed release
		FortiPAM 1.8	Not affected	Not Applicable
		FortiPAM 1.7	1.7.0	Upgrade to 1.7.1 or above
		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 7.6.4	Upgrade to 7.6.5 or above
		FortiProxy 7.4	7.4.0 through 7.4.11	Upgrade to 7.4.12 or above
		FortiProxy 7.2	7.2 all versions	Migrate to a fixed release
		FortiProxy 7.0	7.0 all versions	Migrate to a fixed release
		FortiSwitchManager 7.2	7.2.0 through 7.2.7	Upgrade to 7.2.8 or above
		FortiSwitchManager	7.0.0	Upgrade to

		7.0	through 7.0.6	7.0.7 or above
CVE-2025-61886 (CVSS Score 4.9)	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability [CWE-79] in FortiSandbox and FortiSandbox Cloud may allow an attacker to perform an XSS attack via crafted HTTP requests.	FortiSandbox 5.0	5.0.0 through 5.0.4	Upgrade to 5.0.5 or above
		FortiSandbox 4.4	Not affected	Not Applicable
		FortiSandbox 4.2	Not affected	Not Applicable
		FortiSandbox PaaS 5.0	5.0.0 through 5.0.4	Upgrade to 5.0.5 or above
		FortiSandbox PaaS 4.4	Not affected	Not Applicable
		FortiSandbox PaaS 4.2	Not affected	Not Applicable
CVE-2025-61848 (CVSS Score 6.8)	An improper neutralization of special elements used in an SQL command ('SQL injection') [CWE-89] in FortiAnalyzer, FortiAnalyzer Cloud, FortiManager and FortiManager Cloud may allow an authenticated privileged attacker to execute unauthorized code or commands via crafted requests.	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
		FortiAnalyzer 7.0	7.0 all versions	Migrate to a fixed release
		FortiAnalyzer 6.4	Not affected	Not Applicable
		FortiAnalyzer Cloud 7.6	7.6.0 through 7.6.4	Upgrade to 7.6.5 or above
		FortiAnalyzer Cloud 7.4	7.4.0 through 7.4.8	Upgrade to 7.4.9 or above
		FortiAnalyzer Cloud 7.2	7.2 all versions	Migrate to a fixed release
		FortiAnalyzer Cloud 7.0	7.0 all versions	Migrate to a fixed release
		FortiAnalyzer Cloud 6.4	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
		FortiManager 7.0	7.0 all versions	Migrate to a fixed release
		FortiManager 6.4	Not affected	Not Applicable
		FortiManager Cloud 7.6	7.6.0 through 7.6.4	Upgrade to 7.6.5 or above
		FortiManager Cloud	7.4.0	Upgrade to

		7.4	through 7.4.8	7.4.9 or above
		FortiManager Cloud 7.2	7.2 all versions	Migrate to a fixed release
		FortiManager Cloud 7.0	7.0 all versions	Migrate to a fixed release
		FortiManager Cloud 6.4	Not affected	Not Applicable
CVE-2026-39813 (CVSS Score 9.1)	A Path Traversal vulnerability [CWE-24] in FortiSandbox JRPC API may allow an unauthenticated attacker to bypass authentication via specially 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 4.2	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™.

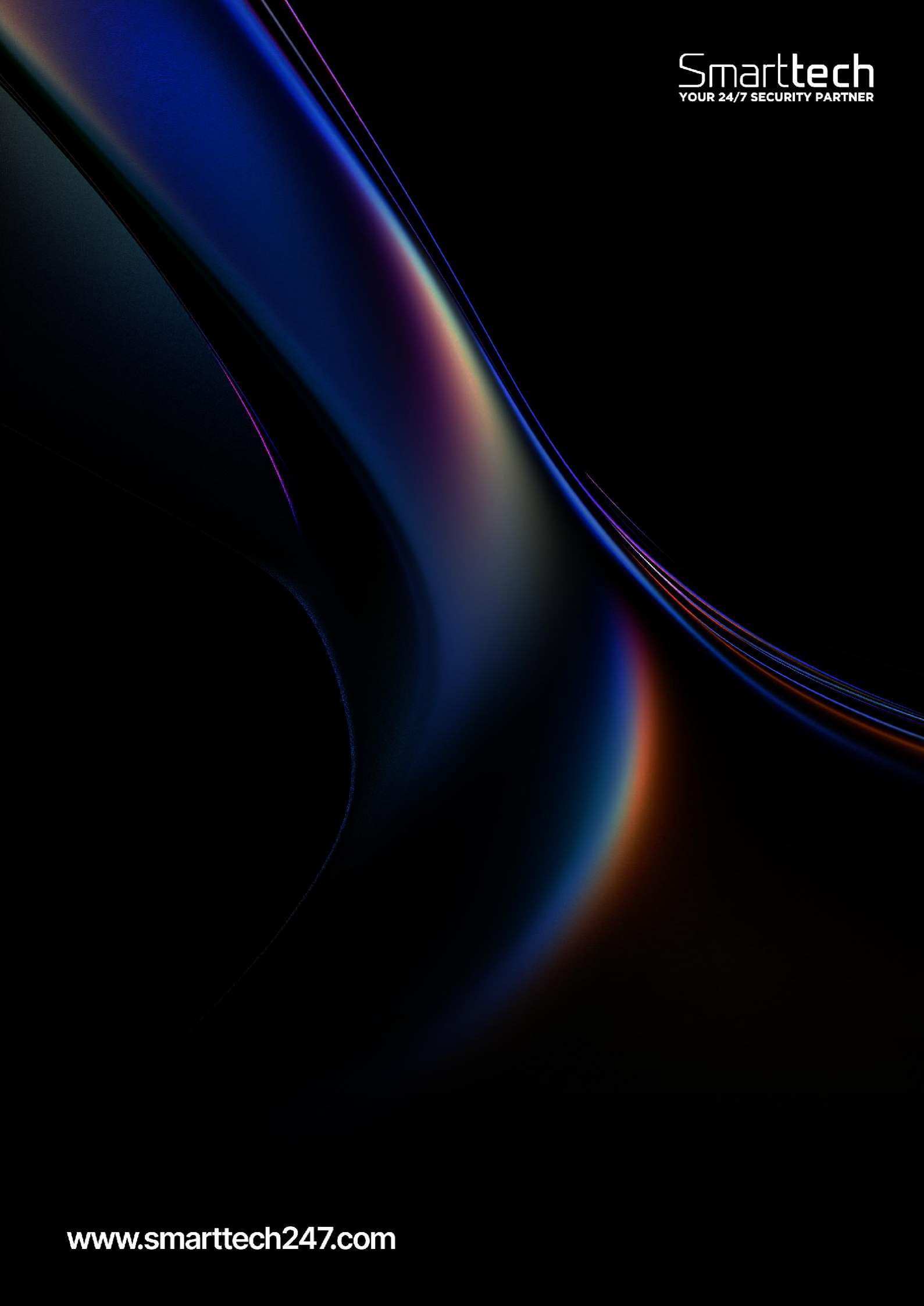
References

https://www.fortiguard.com/psirt/FG-IR-26-115
https://www.fortiguard.com/psirt/FG-IR-26-113
https://www.fortiguard.com/psirt/FG-IR-26-121
https://www.fortiguard.com/psirt/FG-IR-26-125
https://www.fortiguard.com/psirt/FG-IR-26-110
https://www.fortiguard.com/psirt/FG-IR-26-100
https://www.fortiguard.com/psirt/FG-IR-26-120
https://www.fortiguard.com/psirt/FG-IR-26-122
https://www.fortiguard.com/psirt/FG-IR-26-109
https://www.fortiguard.com/psirt/FG-IR-26-111
https://www.fortiguard.com/psirt/FG-IR-26-112

CVEs

CVE-2026-25691
CVE-2026-27316
CVE-2026-22828
CVE-2025-53847
CVE-2026-39812
CVE-2026-39808

CVE-2025-68649
CVE-2025-61624 (Known Exploited)
CVE-2025-61886
CVE-2025-61848
CVE-2026-39813


Smarttech
YOUR 24/7 SECURITY PARTNER
www.smarttech247.com