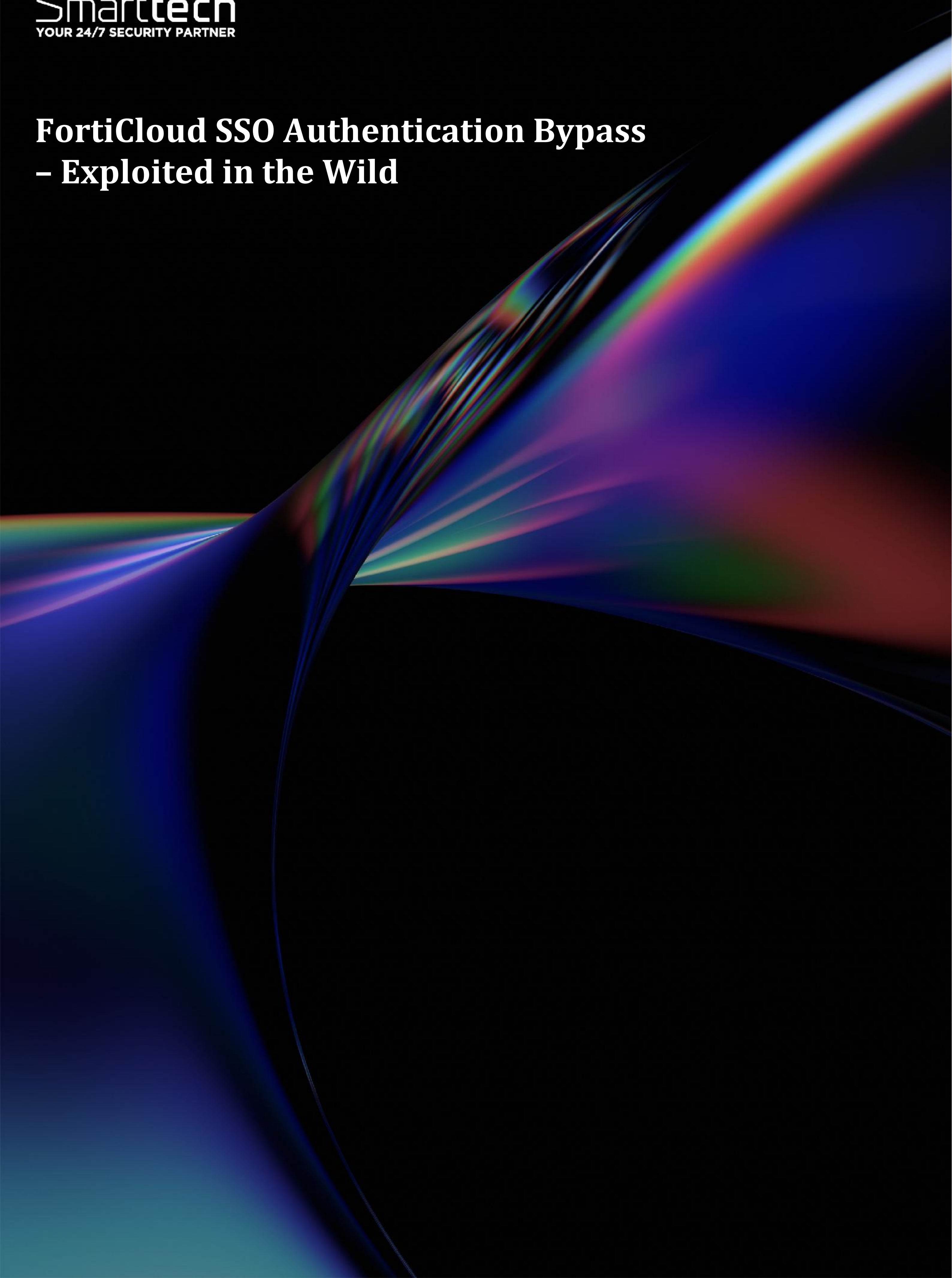
Smarttech
YOUR 24/7 SECURITY PARTNER

FortiCloud SSO Authentication Bypass – Exploited in the Wild



Document ID	SMA-Threat Report
Document status	ISSUED
Issue Number	13
Authors	Dorin Constantin Banu < constantin.banu@smarttech247.com >
Verified by	Alin Curcan < alin.curcan@smarttech247.com >
Last modified	2026-01-28
Issue Date	2026-01-28

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:

A critical severity vulnerability was discovered across several Fortinet products, including FortiOS, FortiManager, FortiAnalyzer, FortiProxy, and FortiWeb. The flaw allows unauthorized access via FortiCloud SSO and it has been confirmed to be actively exploited in the wild.

Risk

Government:

- Large and medium government entities: Critical
- Small government entities: Critical

Businesses:

- Large and medium business entities: Critical
- Small business entities: Critical

Technical summary

CVE ID	CVE Score	Description
CVE-2026-24858	**9.4**	An Authentication Bypass Using an Alternate Path or Channel vulnerability [CWE-288] in FortiOS, FortiManager, FortiAnalyzer may allow an attacker with a FortiCloud account and a registered device to log into other devices registered to other accounts, if FortiCloud SSO authentication is enabled on those devices.

Note: *The FortiCloud SSO login feature is not enabled in default factory settings. It's only turned on in scenarios where an administrator registers the device to FortiCare from the device's GUI, unless they have taken steps to explicitly toggle the "Allow administrative login using FortiCloud SSO" switch.*

Affected Product

Version	Affected	Solution
FortiAnalyzer 7.6	7.6.0 through 7.6.5	Upgrade to upcoming 7.6.6 or above
FortiAnalyzer 7.4	7.4.0 through 7.4.9	Upgrade to 7.4.10 or above
FortiAnalyzer 7.2	7.2.0 through 7.2.11	Upgrade to upcoming 7.2.12 or above
FortiAnalyzer 7.0	7.0.0 through 7.0.15	Upgrade to upcoming 7.0.16 or above
FortiAnalyzer 6.4	Not affected	Not Applicable
FortiManager 7.6	7.6.0 through 7.6.5	Upgrade to upcoming 7.6.6 or above
FortiManager 7.4	7.4.0 through 7.4.9	Upgrade to 7.4.10 or above
FortiManager 7.2	7.2.0 through 7.2.11	Upgrade to upcoming 7.2.13 or above
FortiManager 7.0	7.0.0 through 7.0.15	Upgrade to upcoming 7.0.16 or above

FortiManager 6.4	Not affected	Not Applicable
FortiOS 8.0	Not affected	Not Applicable
FortiOS 7.6	7.6.0 through 7.6.5	Upgrade to upcoming 7.6.6 or above
FortiOS 7.4	7.4.0 through 7.4.10	Upgrade to 7.4.11 or above
FortiOS 7.2	7.2.0 through 7.2.12	Upgrade to upcoming 7.2.13 or above
FortiOS 7.0	7.0.0 through 7.0.18	Upgrade to upcoming 7.0.19 or above
FortiOS 6.4	Not affected	Not Applicable
FortiProxy 7.6	7.6.0 through 7.6.4	Upgrade to upcoming 7.6.6 or above
FortiProxy 7.4	7.4.0 through 7.4.12	Upgrade to upcoming 7.4.13 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

IOC

SSO Login User Accounts

The actor has been observed to have logged in with the following user accounts.

- cloud-noc@mail.io
- cloud-init@mail.io

These addresses may change in the future as action has been taken to neutralize these accounts.

IP Addresses

The actor has been observed to log in via multiple IP addresses and appears to have switched to use Cloudflare protected Ips:

- 104.28.244.115
- 104.28.212.114
- 104.28.212.115
- 104.28.195.105
- 104.28.195.106
- 104.28.227.106
- 104.28.227.105
- 104.28.244.114
- 37.1.209.19
- 217.119.139.50

Malicious Local Account Creation

Following authentication via SSO, it has been observed that the actor creates a local admin account with one of the following names. This has changed through our analysis, so Fortinet recommends reviewing all admin accounts to look for any unexpected entries.

- audit

- backup
- itadmin
- secadmin
- support
- backupadmin
- deploy
- itadmin
- remoteadmin
- security
- svcadmin
- system

Logs

The following log indicates the malicious login event:

```
date=<date> time=<time> devname="FGT60FXXXXXXX" devid=" FGT60FXXXXXXX"
eventtime=<eventtime> tz="<timezone>" logid="0100032001" type="event"
subtype="system" level="information" vd=”root” logdesc="Admin login successful" sn="
FGT60FXXXXXXX" user="cloud-init@mail.io" ui="sso(104.28.244.115)" method="sso"
srcip=104.28.244.115 dstip=<management IP> action="login" status="success"
reason="none" profile="super_admin" msg="Administrator cloud-init@mail.io logged in
successfully from sso(104.28.244.115)"
```

Creation of a local admin, presumably for persistence should the SSO account become disabled, has been seen in almost all cases:

```
date=<date> time=<time> devname="FGT60FXXXXXXX" devid=" FGT60FXXXXXXX"
eventtime=<eventtime> tz="<timezone>" logid="0100044547" type="event"
subtype="system" level="information" vd="root" logdesc="Object attribute
configured" user="cloud-init@mail.io" ui="GUI(104.28.244.115)" action="Add"
cfgtid=<Config ID> cfgpath="system.admin" cfgobj="secadmin" cfgattr="old-
password[]accprofile[super_admin]vdom[root]password[]" msg="Add
system.admin secadmin"
```

Note: *the IOCs in RED may be any of the IOCs listed, however, these have been the most commonly observed at this time.*

Attacker main operations:

- Download customer config file
- Add an admin account to get persistence

Workaround

FortiCloud SSO authentication no longer supports login from devices running vulnerable versions. Therefore, disabling FortiCloud SSO login on client side is not necessary at the moment. For reference, it can nonetheless be done via the following:

- On FortiOS and FortiProxy:
  go to System -> Settings -> Switch "Allow administrative login using FortiCloud SSO" to Off.
  Or type the following command in CLI command line:
  ```
  config system global
      set admin-forticloud-sso-login disable
  end
  ```

- On FortiManager and FortiAnalyzer:
  go to System Settings -> SAML SSO -> Switch "Allow admins to login with FortiCloud" to Off.
  Or type the following command in CLI command line:
  ```
  config system saml
      set forticloud-sso disable
  end
  ```

Post Exploitation Actions

If IOCs are identified in the system, Fortinet recommends treating the system and configuration as compromised and taking the following cleanup actions:

- Ensure your device is running the latest firmware version. It is recommended to run the latest release (7.6) where possible to take advantage of the latest security features.
- Restore your configuration with a known clean version or audit for any unauthorized changes. Pay particular attention to unexpected administrators or VPN configuration or accounts.
- Treat configuration as compromised and follow the guidance below to rotate credentials, including any LDAP/AD accounts that may be connected to the FortiGate devices.

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-26-060
https://www.fortinet.com/blog/psirt-blogs/analysis-of-sso-abuse-on-fortios
https://community.fortinet.com/t5/FortiGate/Technical-Tip-Recommended-steps-to-execute-in-case-of-a/ta-p/230694
https://thehackernews.com/2026/01/fortinet-patches-cve-2026-24858-after.html

CVEs

CVE-2026-24858

Smarttech
YOUR 24/7 SECURITY PARTNER

www.smarttech247.com