CERT-EU

Security Advisory 2025-019

Critical Vulnerabilities in Fortinet Products

2025-05-13 — v1.0

TLP:CLEAR

History:

- *13/05/2025 — v1.0 – Initial publication*

Summary

On 13 May 2025, Fortinet released a security advisory addressing several vulnerabilities in their products, two of which are rated as critical.

It is recommended updating as soon as possible.

Technical Details

The vulnerability **CVE-2025-32756** [1], with a CVSS score of 9.6, is a stack-based overflow vulnerability in FortiFone, FortiVoice, FortiNDR, and FortiMail that could allow a remote unauthenticated attacker to execute arbitrary code or commands via crafted HTTP requests. An unauthenticated attacker could send specific requests to the API endpoint to write arbitrary data outside the bound of the intended buffer and execute arbitrary code or commands.

The vulnerability **CVE-2025-22252** [2], with a CVSS score of 9.0, is a missing authentication for critical function vulnerability in FortiOS, FortiProxy, and FortiSwitchManager TACACS+ configured to use a remote TACACS+ server for authentication, that has itself been configured to use ASCII authentication. This may allow an attacker with knowledge of an existing admin account to access the device as a valid admin via an authentication bypass.

Affected Products

The vulnerability **CVE-2025-32756** affects the following product versions:

- FortiVoice versions 6.4.0 through 6.4.10, 7.0.0 through 7.0.6, and 7.2.0
- FortiRecorder versions 6.4.0 through 6.4.5, 7.0.0 through 7.0.5 and 7.2.0 through 7.2.3
- FortiMail versions 7.0.0 through 7.0.8, 7.2.0 through 7.2.7, 7.4.0 through 7.4.4, and 7.6.0 through 7.6.2
- FortiNDR versions 1.1 to 1.4, 1.5.0 through 1.5.3, 7.0.0 through 7.0.6, 7.1.0 through 7.1.1, 7.2.0 through 7.2.4, 7.4.0 through 7.4.7 and 7.6.0.

The vulnerability **CVE-2025-22252** affects the following product versions:

- FortiOS versions 7.4.4 through 7.4.6, and 7.6.0
- FortiProxy versions 7.6.0 through 7.6.1
- FortiSwitchManager version 7.2.5

This vulnerability is limited to configurations where ASCII authentication is used. PAP, MSCHAP, and CHAP configurations are not impacted.

Recommendations

It is recommended to upgrade to a fixed version as soon as possible.

Workarounds

To mitigate the vulnerability **CVE-2025-32756**, it is possible to disable the web (HTTP/HTTPS) service on the administrative interface [1].

To mitigate the vulnerability **CVE-2025-22252**, it is possible to use an alternate authentication method [2].

Detection

There are several detection opportunities related to the exploitation of **CVE-2025-32756**.

1. Audit logs: the following log entries are indicative of exploitation of the vulnerability

```
Output of CLI command 'diagnose debug application httpd display trace-log':
[x x x x:x:x.x 2025] [fcgid:warn] [pid 1829] [client x.x.x.x:x] mod_fcgid: error reading data,
  FastCGI server closed connection
[x x x x:x:x.x 2025] [fcgid:error] [pid 1503] mod_fcgid: process
  /migadmin/www/fcgi/admin.fe(1741) exit(communication error), get unexpected signal 11
```

2. IP addresses associated to the Threat Actor exploiting this vulnerability:

- `198.105.127[.]124`
- `43.228.217[.]173`
- `43.228.217[.]82`
- `156.236.76[.]90`
- `218.187.69[.]244`
- `218.187.69[.]59`

2. Modified settings:

Verify if `fcgi` debugging is enabled on your system, use the following CLI command:

```
> diag debug application fcgi

fcgi debug level is 0x80041
general to-file ENABLED
```

This is not a default setting, so unless you have enabled it in the past, this is potentially an Indicator of Compromise

3. File modifications:

- [Added File] `/bin/wpad_ac_helper`

- [Added File] `/bin/busybox`
- [Modified File] `/data/etc/crontab`
- [Modified File] `/var/spool/cron/crontabs/root`
- [Added File] `/var/spool/.sync`
- [Modified File] `/etc/pam.d/sshd`
- [Added File] `/lib/libfmlogin.so`
- [Added File] `/tmp/.sshdpm`
- [Added File] `/bin/fmtest`
- [Modified File] `/etc/httpd.conf`

References

[1] https://www.fortiguard.com/psirt/FG-IR-25-254

[2] https://www.fortiguard.com/psirt/FG-IR-24-472