PSIRT

Insertion of sensitive information into REST API logs

IR Number	**FG-IR-24-268**
Published Date	**Dec 9, 2025**
Component	**OTHERS**
Severity	**Medium**
CVSSv3 Score	**6.3**
Impact	**Escalation of privilege**
CVE ID	**CVE-2024-47570**
Download	**CVRF** **CSAF**

Summary

Version	Affected	Solution
FortiOS 7.6	Not affected	Not Applicable
FortiOS 7.4	7.4.0 through 7.4.3	Upgrade to 7.4.4 or above
FortiOS 7.2	7.2.0 through 7.2.7	Upgrade to 7.2.8 or above
FortiOS 7.0	7.0.4 through 7.0.17	Migrate to a fixed release
FortiOS 6.4	Not affected	Not Applicable
FortiPAM 1.7	Not affected	Not Applicable
FortiPAM 1.6	Not affected	Not Applicable
FortiPAM 1.5	Not affected	Not Applicable
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

Version	Affected	Solution
FortiProxy 7.2	7.2.0 through 7.2.11	Upgrade to 7.2.12 or above
FortiProxy 7.0	Not affected	Not Applicable
FortiSASE 24.1	24.1.b	Fortinet remediated this issue in FortiSASE version 24.1.c and hence customers do not need to perform any action.
FortiSRA 1.7	Not affected	Not Applicable
FortiSRA 1.6	Not affected	Not Applicable
FortiSRA 1.5	Not affected	Not Applicable
FortiSRA 1.4	1.4 all versions	Migrate to a fixed release

Follow the recommended upgrade path using our tool at: https://docs.fortinet.com/upgrade-tool

Workarounds:

1. To avoid your tokens being logged when doing API requests, place your API tokens in the request header rather than in the URL.

To pass the API token in the request header, the following field must be added to the request header:
`Authorization: Bearer <YOUR-API-TOKEN>` [1]

2. Disable REST API logs (default setting):

config log setting

Timeline

2025-12-09: Initial publication

References

- [1] Using API tokens with a request header: https://docs.fortinet.com/document/fortigate/7.6.0/administration-guide/940602/using-apis