文書管理番号：SCSK-23125738
2024 年 2 月 9 日

平素より Fortinet 製品をご愛顧いただきありがとうございます。
下記のとおり製品情報及びサポート情報をご案内させて頂きます。

件名： FortiOS - fgfmd におけるフォーマット文字列のバグにおける脆弱性(CVE-2024-23113)
対象製品： FortiGate
CVE ID： CVE-2024-23113
CVSSv3 Score： 9.8
PSIRT リリース日： 2024-2-8

１．概要

FortiOS の fgfmd デーモンに、外部制御されたフォーマット文字列を使用する脆弱性 [CWE-134] があり、リモートの認証されていない攻撃者に、特別に細工されたリクエストを経由して任意のコードまたはコマンドを実行される可能性があります。

２．対象製品バージョン

FortiOS バージョン 7.4.0 ～ 7.4.2
FortiOS バージョン 7.2.0 ～ 7.2.6
FortiOS バージョン 7.0.0 ～ 7.0.13

（FortiOS 6.x は影響を受けません。）

３．対策

以下のバージョンにアップグレードして下さい。
FortiOS バージョン 7.4.3 以降、7.2.7 以降、7.0.14 以降

最新の情報は以下の PSIRT Advisories よりご確認ください。
https://fortiguard.fortinet.com/psirt/FG-IR-24-029

※日本語による情報は、英語による原文の非公式な翻訳となります。
もし、英語原文との間で内容の齟齬がある場合、英語原文が優先されます。

FortiOS - Format String Bug in fgfmd

IR Number	***FG-IR-24-029***
Date	***Feb 8, 2024***
Severity	***Critical***
CVSSv3 Score	***9.8***
Impact	***Execute unauthorized code or commands***
CVE ID	***CVE-2024-23113***
CVRF	***Download***

Summary

A use of externally-controlled format string vulnerability [CWE-134] in FortiOS fgfmd daemon may allow a remote unauthentified attacker to execute arbitrary code or commands via specially crafted requests.

Version	*Affected*	*Solution*
FortiOS 7.4	*7.4.0 through 7.4.2*	*Upgrade to 7.4.3 or above*
FortiOS 7.2	*7.2.0 through 7.2.6*	*Upgrade to 7.2.7 or above*
FortiOS 7.0	*7.0.0 through 7.0.13*	*Upgrade to 7.0.14 or above*

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

FortiOS 6.x is not affected.

Acknowledgement

Internally discovered and reported by Gwendal Guégniaud of Fortinet Product Security team.

以上

SCSK SCSK株式会社