文書管理番号：SCSK-23125756
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 - sslvpnd の境界外書き込みにおける脆弱性(CVE-2024-21762)
対象製品： FortiGate
CVE ID： CVE-2024-21762
CVSSv3 Score： 9.6
PSIRT リリース日： 2024-2-8

１．概要

FortiOS に境界外書き込みの脆弱性 [CWE-787] が存在し、リモートの認証されていない攻撃者が、特別に細工された HTTP リクエストを介して任意のコードまたはコマンドを実行できる可能性があります。

回避策 ：SSL VPN を無効にします (Web モードを無効にすることは有効な回避策ではありません)。
注意: この脆弱性は実際に悪用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 バージョン 6.4.0 ～ 6.4.14
FortiOS バージョン 6.2.0 ～ 6.2.15
FortiOS バージョン 6.0 全バージョン

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、6.4.15 以降、6.2.16 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-24-015

※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 - Out-of-bound Write in sslvpnd

IR Number	***FG-IR-24-015***
Date	***Feb 8, 2024***
Severity	***Critical***
CVSSv3 Score	***9.6***
Impact	***Execute unauthorized code or commands***
CVE ID	***CVE-2024-21762***
CVRF	***Download***

Summary

A out-of-bounds write vulnerability [CWE-787] in FortiOS may allow a remote unauthenticated attacker to execute arbitrary code or command via specially crafted HTTP requests.

Workaround : disable SSL VPN (disable webmode is NOT a valid workaround)

Note: This is potentially being exploited in the wild.

Version	*Affected*	*Solution*
FortiOS 7.6	*Not affected*	*Not Applicable*
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*
FortiOS 6.4	*6.4.0 through 6.4.14*	*Upgrade to 6.4.15 or above*
FortiOS 6.2	*6.2.0 through 6.2.15*	*Upgrade to 6.2.16 or above*
FortiOS 6.0	*6.0 all versions*	*Migrate to a fixed release*

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

以上

SCSK SCSK株式会社