文書管理番号：SCSK-23137864
2024 年 03 月 13 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 & FortiProxy - キャプティブポータルでの境界外書き込み（CVE-2023-42789, CVE-2023-42790）
対象製品： FortiOS, FortiProxy
CVE ID： CVE-2023-42789, CVE-2023-42790
CVSSv3 Score： 9.3
PSIRT リリース日： 2024-03-12

１．概要

FortiOS および FortiProxy のキャプティブポータルに、境界外書き込みの脆弱性 [CWE-787]、およびスタックベースのバッファオーバフロー [CWE-121] があり、キャプティブポータルにアクセスできる内部攻撃者が、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す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 7.4.0～7.4.1
FortiOS バージョン 7.2.0～7.2.5
FortiOS バージョン 7.0.0～7.0.12
FortiOS バージョン 6.4.0～6.4.14
FortiOS バージョン 6.2.0～6.2.15
FortiProxy バージョン 7.4.0
FortiProxy バージョン 7.2.0～7.2.6
FortiProxy バージョン 7.0.0～7.0.12
FortiProxy バージョン 2.0.0 ～ 2.0.13

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 7.4.2 以降、7.2.6 以降、7.0.13 以降、6.4.15 以降、6.2.16 以降
FortiProxy バージョン 7.4.1 以降、7.2.7 以降、7.0.13 以降、2.0.14 以降
フォーティネットは、2023/Q3 に FortiSASE バージョン 23.3.b でこの問題を修正しました。

仮想パッチ「FortiOS.Captive.Portal.Out.Of.Bounds.Write」は、FMWP db update 23.105 で入手可能です。

4. 回避策

フォームベースでない認証スキームを設定する：

config authentication scheme
edit scheme
set method <method>
next
end

ここで、<method>は、以下のいずれでも良い：

・ntlm NTLM 認証
・basic HTTP 認証
・digest HTTP 認証
・negotiate Negotiate 認証
・fsso Fortinet Single Sign-On (FSSO) 認証
・rsso RADIUS シングルサインオン（RSSO）認証
・ssh-publickey 公開鍵ベースの SSH 認証
・cert クライアント証明書認証
・saml SAML 認証

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-23-328

※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 & FortiProxy - Out-of-bounds Write in captive portal

Summary

An out-of-bounds write vulnerability [CWE-787] and a Stack-based Buffer Overflow [CWE-121] in FortiOS & FortiProxy captive portal may allow an inside attacker who has access to captive portal to execute arbitrary code or commands via specially crafted HTTP requests.

Workaround:

Set a non form-based authentication scheme:

config authentication scheme
edit scheme
set method method
next
end

Where <method> can be any of those :

ntlm NTLM authentication.

basic Basic HTTP authentication.

digest Digest HTTP authentication.

negotiate Negotiate authentication.

fsso Fortinet Single Sign-On (FSSO) authentication.

rsso RADIUS Single Sign-On (RSSO) authentication.

ssh-publickey Public key based SSH authentication.

cert Client certificate authentication.

saml SAML authentication

Affected Products

FortiOS version 7.4.0 through 7.4.1
FortiOS version 7.2.0 through 7.2.5
FortiOS version 7.0.0 through 7.0.12

FortiOS version 6.4.0 through 6.4.14

FortiOS version 6.2.0 through 6.2.15

FortiProxy version 7.4.0

FortiProxy version 7.2.0 through 7.2.6

FortiProxy version 7.0.0 through 7.0.12

FortiProxy version 2.0.0 through 2.0.13

Solutions

Please upgrade to FortiOS version 7.4.2 or above

Please upgrade to FortiOS version 7.2.6 or above

Please upgrade to FortiOS version 7.0.13 or above

Please upgrade to FortiOS version 6.4.15 or above

Please upgrade to FortiOS version 6.2.16 or above

Please upgrade to FortiProxy version 7.4.1 or above

Please upgrade to FortiProxy version 7.2.7 or above

Please upgrade to FortiProxy version 7.0.13 or above

Please upgrade to FortiProxy version 2.0.14 or above

Fortinet in Q3/23 has remediated this issue in FortiSASE version 23.3.b and hence the customers need not perform any action.

Virtual Patch named "FortiOS.Captive.Portal.Out.Of.Bounds.Write." is available in FMWP db update 23.105

Acknowledgement

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

Timeline

2024-02-27: Initial publication

以上

SCSK SCSK株式会社