文書管理番号：SCSK-23070818
2023 年 06 月 26 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： FortiNAC - Java の信頼できないオブジェクトのデシリアライゼーション RCE（CVE-2023-33299）
対象製品： FortiNAC
CVE ID： CVE-2023-33299
CVSSv3 Score： 9.6
PSIRT リリース日： 2023-6-23

１．概要
FortiNAC における信頼できないデータのデシリアライゼーションの脆弱性 [CWE-502] により、認証されていないユーザが、tcp/1050 サービスに対する特別に細工されたリクエストを経由して、認証されていない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
FortiNAC バージョン 9.4.0 ～ 9.4.2
FortiNAC バージョン 9.2.0 ～ 9.2.7
FortiNAC バージョン 9.1.0 ～ 9.1.9
FortiNAC バージョン 7.2.0 ～ 7.2.1
FortiNAC 8.8 すべてのバージョン
FortiNAC 8.7 すべてのバージョン
FortiNAC 8.6 すべてのバージョン
FortiNAC 8.5 すべてのバージョン
FortiNAC 8.3 すべてのバージョン

３．対策
以下のバージョンにアップグレードして下さい。
FortiNAC バージョン 9.4.3 以降、9.2.8 以降、9.1.10 以降、7.2.2 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-23-074

※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。

FortiNAC - java untrusted object deserialization RCE

Summary

A deserialization of untrusted data vulnerability [CWE-502] in FortiNAC may allow an unauthenticated user to execute unauthorized code or commands via specifically crafted requests to the tcp/1050 service.

Affected Products

FortiNAC version 9.4.0 through 9.4.2

FortiNAC version 9.2.0 through 9.2.7

FortiNAC version 9.1.0 through 9.1.9

FortiNAC version 7.2.0 through 7.2.1

FortiNAC 8.8 all versions

FortiNAC 8.7 all versions

FortiNAC 8.6 all versions

FortiNAC 8.5 all versions

FortiNAC 8.3 all versions

Solutions

Please upgrade to FortiNAC version 9.4.3 or above

Please upgrade to FortiNAC version 9.2.8 or above

Please upgrade to FortiNAC version 9.1.10 or above

Please upgrade to FortiNAC version 7.2.2 or above

Acknowledgement

Fortinet is pleased to thank Florian Hauser from CODE WHITE for reporting this vulnerability under responsible disclosure.

Timeline

2023-06-19: Initial publication

以上

SCSK株式会社
ネットワークセキュリティ事業本部
カスタマーサポート部