

文書管理番号 : SCSK-23071204

2023 年 6 月 30 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いただきます。

件名 : 証明書バンドル 1.00044 (CRDB) アップデートによる Web サイトのブロック

対象製品 : FortiOS v6.0 および v6.2 が動作する FortiGate

Customer Support Bulletin : CSB-230629-1

CSB リリース日 : 2023-06-29

1. 概要

フォーティネットは、FortiGuard Distribution Network の証明書バンドル (CRDB) のアップデート (バージョン 1.00044) をリリースしました。このリリースには、Fortinet_Wifi_CA 認証局への更新が含まれており、FortiOS v6.0 および v6.2 で SSL ハンドシェイクが処理されないケースが発生する可能性があります。

2. 対象製品バージョン

FortiOS v6.2, v6.0

3. 対策

フォーティネットは、2023 年 6 月 29 日に証明書チェーンを修正した新しい証明書バンドル、バージョン 1.00045 をリリースしました。以下のコマンドを実行し、FortiGate がパッチを適用した CRDB バージョンであることを確認してください。

```
# execute update-now  
# diagnose autoupdate versions | grep -A6 "Certificate Bundle"
```

4. 回避策

CRDB バージョン 1.00044 の FortiGate では、トラフィックが少ない時間帯に FortiOS の fnbamd と wad を再起動する必要があります。

```
# fnsysctl killall fnbamd  
# diagnose test application wad 99
```

すでに CRDB 1.00044 で回避策を適用しているお客様は、1.00045 へのアップデート後に再度回避策を実行する必要があります。そうしないと、"DigiCert Global G2 TLS RSA SHA256 2020 CA1 "で署名された Web サーバーへのアクセスに問題が発生する可能性があります。

※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。

Certificate Bundle 1.00044 (CRDB) Update Blocking Web Sites

2023-06-29

Subject: Certificate Bundle 1.00044 (CRDB) Update Blocking Web Sites

Released: 2023-06-29

Modified: 2023-06-29

Product: FortiGate firewalls running FortiOS 6.0 and 6.2.

Description:

Fortinet released an update, version 1.00044, to the certificate bundle (CRDB) to the FortiGuard Distribution Network. The release included an update to the Fortinet_Wifi_CA certificate authority, which may result in an unhandled SSL handshaking case by FortiOS v6.0 and 6.2

Affected Products:

FortiGate firewalls running FortiOS 6.0 and 6.2.

Affected OS:

FortiOS 6.0 and 6.2

Resolution:

Fortinet released a new certificate bundle, version 1.00045, with a corrected certificate chain on June 29, 2023. Execute the commands below to ensure the FortiGate is on the patched CRDB version.

```
# execute update-now
```

```
# diagnose autoupdate versions | grep -A6 "Certificate Bundle"
```

Workaround:

FortiGate on CRDB version 1.00044 will require restarting fnbamd and wad in FortiOS at a time of low traffic

```
# fnsysctl killall fnbamd
```

```
# diagnose test application wad 99
```

The customers who have already applied the workaround on the CRDB 1.044, will require to run the workaround again after updating to 1.045, otherwise, you may encounter access problems to web servers signed by "DigiCert Global G2 TLS RSA SHA256 2020 CA1"

以上

SCSK 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