



FutureNet NXR,WXRシリーズにおける再帰的名前解決を行う DNSリゾルバの実装に名前解決を無限に繰り返す問題について

[脆弱性情報]

弊社FutureNet NXR,WXRシリーズは、JVNVU#91812636で報告されている「再帰的名前解決を行うDNSリゾルバの実装に名前解決を無限に繰り返す問題」に該当致します。

[対象製品]

FutureNet NXR-1200

FutureNet NXR-350/C

FutureNet NXR-230/C

FutureNet NXR-155/Cシリーズ

FutureNet NXR-130/C

FutureNet NXR-125/CX

FutureNet NXR-120/C

FutureNet WXR-250

FutureNet NXR-G100シリーズ

[参考情報]

<http://jvn.jp/vu/JVNVU91812636/index.html>

[対策ファームウェア]

本脆弱性の対策を施したファームウェアをダウンロードし、バージョンアップをおこなってください。

FutureNet NXR-1200 Ver5.25.8で対応

FutureNet NXR-350/C Ver5.26.7で対応

FutureNet NXR-230/C Ver5.26.5で対応

FutureNet NXR-125/CX Ver5.25.7で対応

FutureNet NXR-120/C Ver5.25.7で対応

FutureNet WXR-250 Ver1.4.0で対応

FutureNet NXR-G100シリーズ Ver6.5.3で対応

その他製品のファームウェアは、順次公開予定です。

[該当している場合の影響を軽減する方法]

- DNSのルートサーバへのアクセスを無効にする。(デフォルト値は無効)
- DNS設定のlimitation enableによりアクセスするDNSサーバを制限する。

※limitation enableコマンドを設定することにより、指定DNSサーバ以外への再帰問い合わせを行わなくなります。

- 事象発生時にclear dns cacheコマンドおよびrestart dnsコマンドを実行する。

[更新履歴]

2014/12/26 新規登録

2015/01/29 NXR-230/C対応

2015/02/05 NXR-G100シリーズ対応

2015/02/20 NXR-125/CX対応

2015/04/02 NXR-1200対応

2015/04/09 NXR-120/C対応

2015/09/09 NXR-350/C対応

2016/02/01 WXR-250対応