

2011 年 10 月 31 日

お客様各位

パナソニック ソリューションテクノロジー株式会社
ソフトウェアグループ プロダクト1 チーム

Apache HTTPD サーバの Range ヘッダーの DoS 脆弱性について

拝啓 貴社ますますご清栄のことと、お慶び申し上げます。

さて、この度 Web サーバーソフトウェアの Apache に関して、一般社団法人 JPCERT コーディネーションセンターが緊急の脆弱性を公開しました。この脆弱性は遠隔の第三者によって、サービス運用妨害 (DoS) 攻撃を受ける可能性があり、"Apache Killer" と呼ばれる攻撃ツールの公開も確認しております。

内容を確認の上、必要に応じて対策を実施頂きますようお願い申し上げます。

敬具

—記—

1. 対象製品

以下製品の Web サーバでご利用されている Apache のバージョンにより影響がございます。

- GlobalDoc5、GlobalFlow5、GlobalSchedule5
- GlobalWare
- GlobalDoc Lite、GlobalFlow Lite
- GlobalPortal
- Mobile Gateway
- リアルタイムコラボレーション
- 機密文書管理 (GlobalDoc SAFER)

2. 環境構築用インストール CD-ROM に同梱されている Apache Ver.2.0.x ~ Ver.2.0.65 までをご利用のお客様

対応方法

Apache の設定ファイル httpd.conf に以下の行を追加し、Web サービスを再起動します。

```
=====
# Reject request when more than 5 ranges in the Range: header.
# CVE-2011-3192
RewriteEngine on
RewriteCond %{HTTP:range} !(bytes=[^,]+(,[^,]+){0,4}$|^$)
RewriteRule .* - [F]
# We always drop Request-Range; as this is a legacy
# dating back to MSIE3 and Netscape 2 and 3.
RequestHeader unset Request-Range
=====
```

3. 環境構築用インストール CD-ROM に同梱されている Apache Ver.2.2.x ~
Ver.2.2.20 までをご利用のお客様

対応方法

Apache の設定ファイル httpd.conf に以下の行を追加し、Web サービスを再起動します。

```
=====
# Drop the Range header when more than 5 ranges.
# CVE-2011-3192
SetEnvIf Range (?:,*?){5,5} bad-range=1
RequestHeader unset Range env=bad-range
# We always drop Request-Range; as this is a legacy
# dating back to MSIE3 and Netscape 2 and 3.
RequestHeader unset Request-Range
# optional logging.
CustomLog logs/range-CVE-2011-3192.log common env=bad-range
CustomLog logs/range-CVE-2011-3192.log common env=bad-req-range
=====
```

4. 参考情報

情報源については、以下をご確認ください。

Japan Vulnerability Notes JVN#405811 (2011年10月31日時点)

Apache HTTPD サーバにサービス運用妨害 (DoS) の脆弱性

<https://jvn.jp/cert/JVN#405811/>

以上