

Sendmail における新たな脆弱性について

拝啓、貴社益々ご清栄の事とお喜び申し上げます。  
平素は格別なるご高配を賜りまして、厚く御礼申し上げます。

この度、Sendmail のメールヘッダーの処理に、スタックバッファオーバーフローの脆弱性が存在することが、3 月 29 日付けで CERT-CC より報告されました。

この脆弱性は、3 月 4 日に報告された sendmail の情報(CVE コード:CAN-2002-1337)とは異なるものです。

つきましては、診断結果に下記の脆弱性が検出されていないかをご確認ください。

敬具

記

【Sendmail のバッファオーバーフロー脆弱性】

(CVE ID : CAN-2003-0161)

QualysID 74136 :

「Sendmail Address Prescan Possible Memory Corruption Vulnerability」

[本脆弱性の対象]

- Sendmail Pro (すべてのバージョン)
- Sendmail Switch 2.1 (2.1.6 より前のバージョン)
- Sendmail Switch 2.2 (2.2.6 より前のバージョン)
- Sendmail Switch 3.0 (3.0.4 より前のバージョン)
- Sendmail for NT 2.X (2.6.3 より前のバージョン)
- Sendmail for NT 3.0 (3.0.4 より前のバージョン)
- Systems running open-source sendmail (8.12.9 より前のバージョン) , UNIX および Linux を含む
- Sendmail Advanced Message Server (これは Sendmail Switch を含む)

[対処について]

- 商用版の場合  
ベンダーのパッチを適用します。  
<http://www.sendmail.com/security/>

- オープンソース版の場合

- ・ 8.12.9 に更新します。
- ・ または、パッチを適用します。

vulnwatch に [sendmail.org](http://www.sendmail.org) が投稿したメールには、8.12.x, 8.11.x, 8.9.x 用のパッチが添付されています。

\* 修正プログラムについての注意 \*

概要において述べているように、今回のセキュリティ脆弱性を攻略する攻撃は、内部メールサーバーも標的となるため、8.12.9 の修正プログラムには、内部メールサーバーを保護するために、次の処置もなされています。

- ・ メールヘッダなどに含まれる (char) 0xff を (char) 0x7f に変換する。
- ・ MaxMimeHeaderLength を 2048/1024 に変更している。

これらの処理によって、外部メールサーバーを更新(または修正プログラムを適用)することにより、外部からの攻撃メールを無力化することができます。しかし、このヘッダー改変や長さ制限によって別の問題が発生する場合、この保護機能を無効化することもできます。

また、修正プログラムについては、PGP または GnuPG により、デジタル署名を検証することをお勧めします。

詳細については、<http://www.sendmail.org/patchps.html> を参照してください。

[関連文書]

Qualys セキュリティアラート

Qualys Provides Security Test for Latest Vulnerability in SENDMAIL

[http://www.qualys.com/news/pr/index.php?page=pr\\_03\\_30\\_03&lk=hm\\_pg](http://www.qualys.com/news/pr/index.php?page=pr_03_30_03&lk=hm_pg)

JPCERT/CC Alert 2003-03-31

新たな sendmail の脆弱性に関する注意喚起

<http://www.jpccert.or.jp/at/2003/at030004.txt>

-以上-

-----  
お問い合わせ窓口)

富士通株式会社

システムサポート本部セキュリティサービス統括部セキュリティシステム部

[qualys-support@support.fujitsu.com](mailto:qualys-support@support.fujitsu.com)

担当：長谷川、安立、松本

電話：044-754-3353