

アタックテストサービス エクスプレスご利用のお客様へ

平成 16 年 7 月 5 日
富士通株式会社

7 月 2 日発表の Download.Ject における脆弱性について

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、「Download.Ject における脆弱性」に関する情報が 7 月 2 日付けで Qualys 社より報告されました。

下記の方法に従って、QualysGuard で本脆弱性が検出されないかをご確認ください。万が一検出された場合には、至急対処のご検討をしていただきますようお願いいたします。

敬具

記

【Download.Ject における脆弱性】

QualysID : 90131

「Microsoft Internet Explorer Critical Patch KB870669 Missing」

現在、鋭意和訳中です。近日中に和訳を公開いたします。

[脆弱性の詳細について]

マイクロソフト社は、Download.Ject として知られている Internet Explorer の脆弱性を悪用する攻撃への対応として Windows XP、Windows 2000、Windows Server 2003 の設定を変更するための緊急パッチを発表しました。

この脆弱性は、先週多数のウェブサイトを通して Scob（トロイの木馬）を拡散させるために利用され、世間の注目を集めました。

[関連 URL]

・ Download.Ject に関する情報

（日本文）

http://www.microsoft.com/japan/security/incident/download_ject.msp

（英文）

<http://www.microsoft.com/presspass/press/2004/jul04/07-02configchange.asp>

・ Qualys セキュリティアドバイザリ（英文）

Microsoft Update: New Critical Patch to Protect Against Download.Ject Vulnerability

<http://www.qualys.com/research/alerts/view.php/2004-07-02>

[確認方法]

以下の方法にて、本脆弱性のみを選択して短時間で診断することが可能です。

- 1) QualysGuard にログインし、"Preferences"->"Options"->"Profiles"より"New Profile" を作成します。
- 2) "Vulnerability Detection"オプションの「Custom」を選択し、"Configure..."をクリックします。

Find を「QID」, within を「All」, containing を「90131」として"Search"し、QualysID「90131」を選択して"OK"してください。

もし、Windows(NetBIOS)マシン名でホストの脆弱性を調査したい時には、QualysID「82044」(『Windows ホスト名』)も選択してください。

- 3) "Profile Title"をつけ、最後に"Save"します。

- 4) "Scan"->"Launch Scan"で診断対象の IP を選択し、先程作成した"Options"を選択し、"Start Scan"します。

- 以上 -

お問い合わせ窓口)

富士通株式会社 アウトソーシング事業本部

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

<http://segroup.fujitsu.com/secure/service/attacktest-express/index.html>

担当：内田、長谷川、松本、市川