HTTP TRACE メソッドの現状

2011/04/13

HTTP TRACE メソッドの脆弱性は、Cross-Site Tracing という名前で広く知れ渡っています。攻撃が公開されたのは 2003 年 1 月で、POC(サンプル)コードも公開されているものの、未だに悪用された実例のない脆弱性です。悪用された場合は、Web ブラウザがサイトにアクセスする際に自動的に付加する Cookie や Basic 認証が漏洩します。

対策は Web ブラウザと Web サーバの両方で行われています。Web サーバ側では、Microsoft の IIS では 6.0 以降で TRACE メソッド自体が利用できなくなっています。Apache HTTPD についてはデフォルトで利用できますが、設定を変更することにより利用できなくなります。Apache Tomcat は 5.5 以降でデフォルトの設定で利用できません。つまり、**Web サーバ側では一番利用されている Apache HTTPD 及び Apache HTTPD ベースの他のソフトウェアで、TRACE メソッドが利用できる状態となっています。**

では、Web ブラウザはどのソフトウェアのどのバージョンで利用できるのでしょうか。利用率が 1 位 Internet Explorer、2 位の Firefox、Chrome、Safari、Opera 及び Netscape について、どのバージョンで TRACE メソッドが利用可能で、利用率はどの程度あるのかの調査を行いました。以下の表は調査結果です。尚、利用率は TRACE メソッドが利用可能なブラウザのみ調査を行いました。

表 1 Internet Explorer における TRACE メソッド利用の可/不可

ブラウザ	製品発売日	利用率	TRACE メソッド
Internet Explorer 5.0	1998/09/18	0%	○ (※3)
Internet Explorer 5.5 Service Pack 1	2000/11/02	0%	○ (※3)
Internet Explorer 6.0	2001/12/31	10%	○ (※3)
Internet Explorer 6.0 Service Pack 1	2002/09/18		○ (※3)
Internet Explorer 6.0 Service Pack 2 (※1)	2004/09/17		○ (※3) (※4)
Internet Explorer 6.0 Service Pack 3 (※2)	2008/04/21		×
Internet Explorer 7	2006/10/18	－	×
Internet Explorer 8	2009/06/17	－	×

(※1) Windows XP Service Pack 2 に同梱

(※2) Windows XP Service Pack 3 に同梱

(※3) localhost からすべての FQDN 又は同一 FQDN でのみ利用可能

(※4) メソッドを「¥nTRACE」とした場合に利用可能

表 2 Firefox における TRACE メソッド利用の可/不可

ブラウザ	公開日	利用率	TRACE メソッド
Firefox 1.0.4	2005/05/12	0%	○ (※1)
Firefox 1.0.5	2005/07/12		○ (※1)
Firefox 1.0.6	2005/07/20		○ (※1)
Firefox 1.0.7	2005/09/21		○ (※1)
Firefox 1.5	2005/11/29	－	×
Firefox 4.0	2011/03/22		×

(※1) 同一 FQDN でのみ利用可能

表 3 Chrome における TRACE メソッド利用の可/不可

ブラウザ	公開日	利用率	TRACE メソッド
Chrome 1.0.154.36 (※)	2008/12/12	－	×
Chrome 10.0.648.204	2011/03/24		×

(※) 最初の正式版のリリース

表 4 Safari における TRACE メソッド利用の可/不可

ブラウザ	公開日	利用率	TRACE メソッド
Safari 3.1 (※)	2008/03/18	－	×
Safari 4.0	2009/06/18		×
Safari 5.0	2010/06/08		×

(※) Windows 版の最初の正式版のリリース

表 6 Opera における TRACE メソッド利用の可/不可

ブラウザ	公開日	利用率	TRACE メソッド
Opera 7.5	2004/03/12	－	－ (※1)
Opera 8.0	2005/04/18		× (※2)
Opera 8.5	2005/09/20		× (※2)
Opera 9.0	2006/06/20		× (※2)
Opera 10.0	2009/09/01		× (※2)
Opera 11.01	2011/01/27		×

(※1) XMLHttpRequest オブジェクトの未サポート

(※2) TRACE メソッド等は GET メソッドに置換されて同一 FQDN でのみ実行

表 5 Netscape における TRACE メソッド利用の可/不可

ブラウザ	公開日	利用率	TRACE メソッド
Netscape 7.0	2002/08/29	0%	△ (※1)
Netscape 8.0.2	2005/06/16		△ (※1)
Netscape 9.0.0.6 (※2)	2008/02/20		△ (※1)

(※1) 同一 FQDN でのみ利用可能

(※2) 最後のリリース

ここで問題となるブラウザは、TRACE メソッドが利用可能なブラウザの内、未だ利用されている可能性のある Internet Explorer 6.0 です。localhost からの利用は実質不可能であったとしても、同一 FQDN 内での利用は考えられます。Internet Explorer 6.0 の Service Pack の適用状況までは Web サイトのアクセス解析から分からない為、Internet Explorer 6.0 Service Pack 2 及びそれ以前のブラウザが利用されている可能性もあります。

TRACE メソッドが利用可能かどうかはこれ以上分からない為、ブラウザのサポート期限の調査を行ってみました。調査した結果、Internet Explorer 6.0 の内、Service Pack 3 以外はすでにサポート終了となっていました。最後にサポート終了となった Service Pack 2 のサポート終了日は 2010 年 7 月 13 日です。また、Firefox についても 1.5 及びそれ以前のバージョンのサポートはすでに終了しています。Netscape もすべてのバージョンのサポートは 2008 年 2 月 1 日で終了しています。つまり、サポートのある Web ブラウザで TRACE メソッドが利用可能なブラウザは、ほぼ存在しないということです。

上記の結果より、**ブラウザ側では、サポートのあるブラウザはほぼ全て TRACE メソッドの利用はできない状況となっていますが、サポートが終了し、かつ同一 FQDN 内からのみ TRACE メソッドが利用できるブラウザは極僅ですが利用されている可能性があります。**

上記の結果を受け、それぞれの立場の方が適切な判断をして頂ければと思います。

筆者：白石　雅