NTTデータ・セキュリティ株式会社

AWStats のクロスサイトスクリプティングの脆弱性に関する検証レポート

2008/9/25
診断ビジネス部
辻　伸弘
松田　和之

【概要】

AWStats の awstats.pl のパラメータ処理にクロスサイトスクリプティングの脆弱性が発見されました。
この脆弱性により、悪意のあるユーザが細工した URL へサイト利用者を誘導することで Cookie（セッション情報やパスワードなど）が漏洩する危険性があります。漏洩した情報により、悪意のあるユーザはなりすましを行うことが可能となります。

AWStats は、Web サーバのアクセスログを解析し、ブラウザで統計情報を閲覧可能にするプログラムです。
アクセス統計のため、提供している Web サービスと同一のサイトに、AWStats が設置され、インターネットから閲覧可能であるシステムも想定されます。この場合、提供中の Web サービスにクロスサイトスクリプティングの脆弱性が存在しない場合でも、AWStats の脆弱性を利用されることにより、当該サイトで利用している Cookie を窃取される危険性があるため、注意が必要です。

今回、AWStats のクロスサイトスクリプティングの脆弱性についての検証を行いました。

【影響を受けるとされているシステム】

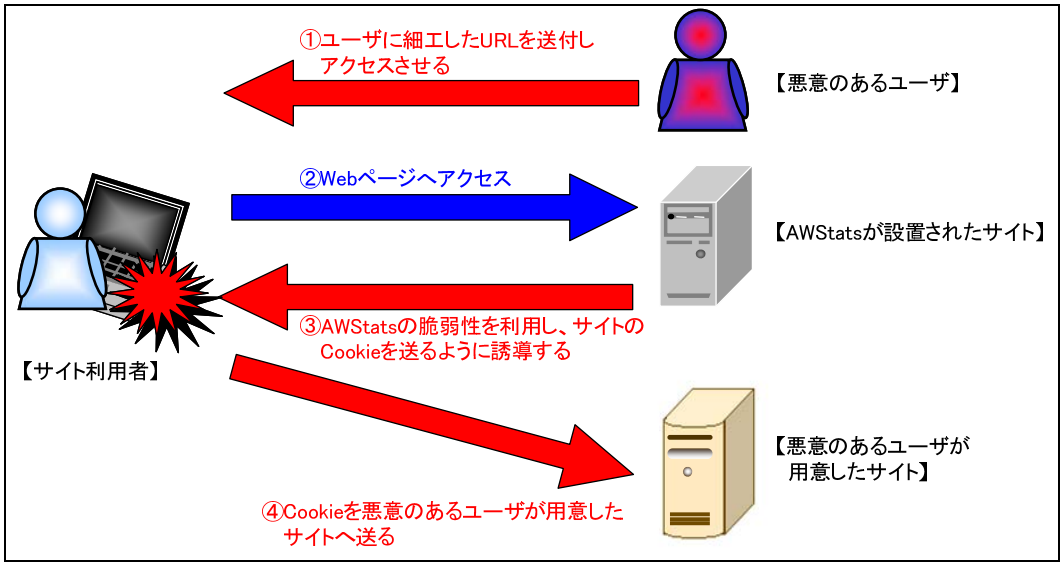
AWStats 6.8

【対策案】

修正されたバージョン「AWStats 6.9」がリリースされております。
修正されたバージョンにアップデートすることが推奨されます。
http://awstats.sourceforge.net/#DOWNLOAD

また、AWStats へアクセスする必要のある接続元からしか接続できないよう、AWStats が設置されたディレクトリへのアクセス制限を実施することが推奨されます。

【被害イメージ】



【検証ターゲットシステム】

AWStats 6.8 がインストールされた CentOS 5

【検証概要】

サイト利用者に、悪意のあるユーザが細工した URL にアクセスさせることで、脆弱性を含む AWStats が設置されたサイトの Cookie を取得します。
今回の検証に用いたスクリプトは、脆弱性を含む AWStats が設置されたサイトで利用している Cookie を、悪意のあるユーザが用意したサイトへ送信するものです。(「被害イメージ」参照)

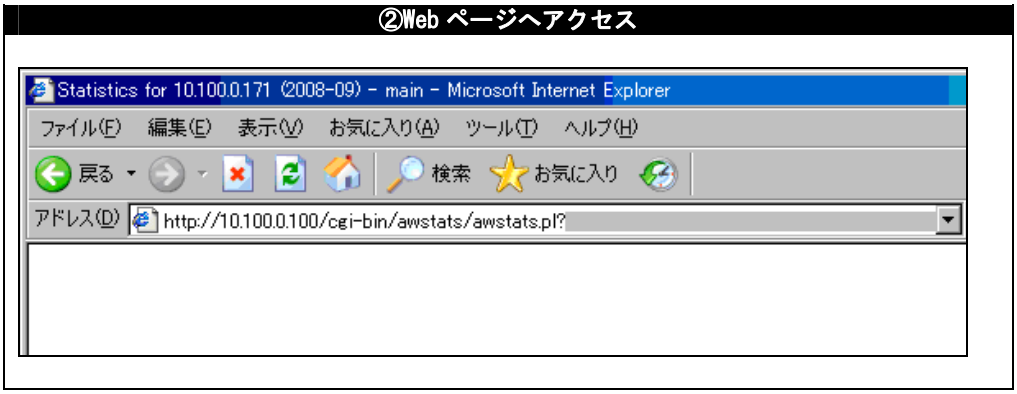
【検証結果】

以下に、被害イメージの流れに沿って検証を行いました。

検証結果中のブラウザに表示されているアドレスは下記の意味を持っています。

10.100.0.50 : 悪意のあるユーザが用意したサイト
10.100.0.100 : 脆弱性を含む AWStats が設置されたサイト

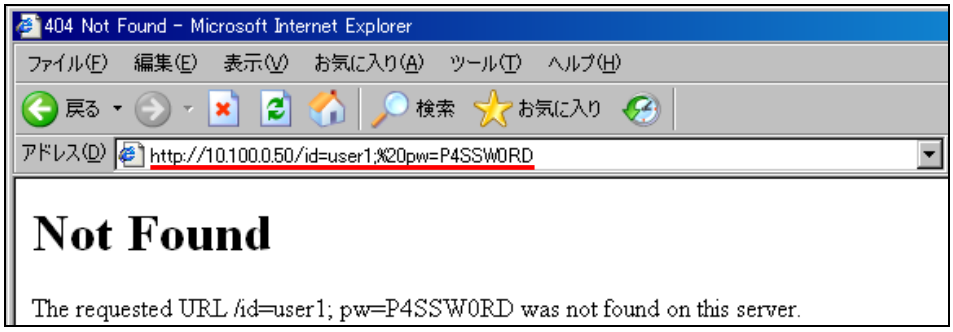
まず、悪意あるユーザは、メール・掲示板などで、サイト利用者に細工した URL を通知し、アクセスするように誘導します。
(被害イメージ①)



上図は、サイト利用者が、悪意のあるユーザが細工した URL にアクセスした画面を示しています。
(被害イメージ②)

この段階で、AWStats が設置されたサイトで使用されている Cookie が読み出されます。
サイト利用者が細工された URL にアクセスすることで、AWStats の脆弱性を利用され、悪意のあるユーザが用意したサイトへ Cookie を送信するよう誘導させられます。
(被害イメージ③)

④Cookie を悪意のあるユーザが用意したサイトへ送る



上図は、スクリプトにより、自動的に悪意のあるユーザが用意したサイトへ、AWStats が設置されたサイトで利用している Cookie を URL に付加してアクセスさせられた際の画面を示しています。
（被害イメージ④）

悪意のあるユーザが用意したサイトのアクセスログ

```
10.100.0.118 - - [25/Sep/2008:14:39:41 +0900] "GET / HTTP/1.1" 200 455 "-" "Mozilla/4.0 (c
ompatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322; InfoPath.1; .NET CLR 2.0.5072
7)"
10.100.0.118 - - [25/Sep/2008:14:40:29 +0900] "GET /index.php HTTP/1.1" 404 284 "-" "Mozil
la/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322; InfoPath.1; .NET CLR
 2.0.50727)"
10.100.0.118 - - [25/Sep/2008:14:40:33 +0900] "GET /index.php HTTP/1.1" 404 284 "-" "Mozil
la/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322; InfoPath.1; .NET CLR
 2.0.50727)"
10.100.0.118 - - [25/Sep/2008:14:41:48 +0900] "GET /id=user1;%20pw=P4SSW0RD HTTP/1.1" 404
296 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322; InfoPa
th.1; .NET CLR 2.0.50727)"
```

上図の赤線で示したとおり、悪意のあるユーザが用意したサイトのアクセスログに、信頼できるサイトの Cookie が記録されていることを示しています。このように、悪意のあるユーザは、取得した Cookie を利用し、なりすましを行うことが可能であると判断できます。

【対策案】

修正されたバージョン「AWStats 6.9」がリリースされております。
修正されたバージョンにアップデートすることが推奨されます。
http://awstats.sourceforge.net/#DOWNLOAD

また、AWStats へアクセスする必要のある接続元からしか接続できないよう、AWStats が設置されたディレクトリへのアクセス制限を実施することが推奨されます。

【参考サイト】

CVE-2008-3714
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3714

＊各規格名、会社名、団体名は、各社の商標または登録商標です。

【お問合せ先】
NTT データ・セキュリティ株式会社
営業企画部
TEL:03-5425-1954
http://www.nttdata-sec.co.jp/