NTTデータ・セキュリティ株式会社

XOOPS のディレクトリトラバーサルの脆弱性に関する検証レポート

2008/12/15
診断ビジネス部
辻　伸弘
松田　和之

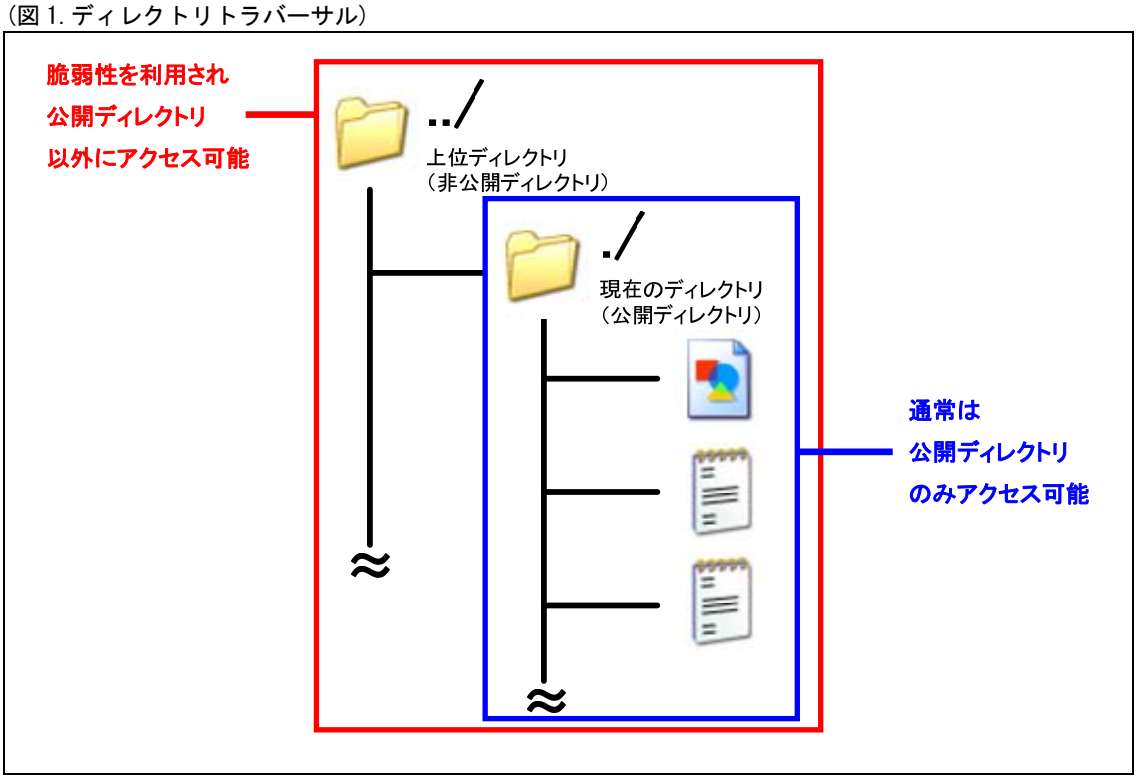
【概要】

XOOPS のローカルファイルインクルード処理に欠陥があり、ディレクトリトラバーサル攻撃を受ける脆弱性が発見されました。この脆弱性により、細工されたリクエストを送信することで、ターゲットシステムの任意のローカルファイルが閲覧可能となります。

ローカルインクルードとは、プログラムにおいて、別ファイルを読み込み、機能をひとつにまとめるために利用される機能です。
また、ディレクトリトラバーサル攻撃とは、相対パス（現在位置を基点として目的位置までのパスを記述する記述方法）を利用して、Web サーバ上で公開している以外の、管理者が意図しないディレクトリ、及び、ファイルにアクセスする攻撃手法です。

通常、Web サーバでは、設定されている公開ディレクトリ以外にアクセスを行うことはできません。(図 1. 青枠部分)
しかし、ディレクトリトラバーサルの脆弱性を利用することで、システム内の重要情報を含むファイルやディレクトリが存在する非公開のディレクトリやファイル（図 1. 赤枠部分）へのアクセスが可能となります。
脆弱性を利用し、本来アクセス不可能なディレクトリへと横断（トラバーサル:traversal)、アクセスすることからディレクトリトラバーサルと呼ばれています。

(図 1. ディレクトリトラバーサル)



想定される被害としては、悪意のあるユーザにより、Web サーバ上で公開しているファイル以外のシステムの固有情報を含むファイル等が漏洩することが挙げられます。

今回、この脆弱性の再現性について検証を行いました。

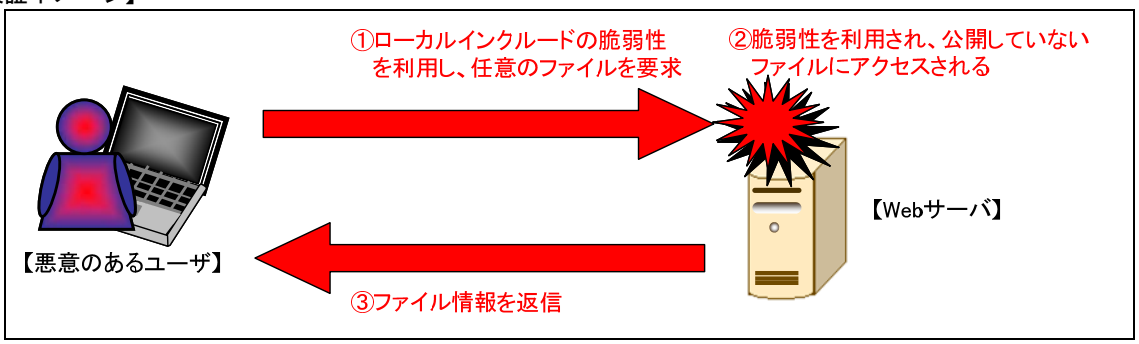
【影響を受けるとされているシステム】
XOOPS 2.3.1 を利用していて、かつ、PHP が以下の設定の場合に影響を受けます。
・register_globals が有効である（register_globals = On）

【対策案】
最新バージョン（XOOPS 2.3.2b）へアップデートすることが推奨されます。
http://www.xoops.org/modules/news/article.php?storyid=4563

また、PHP の設定ファイル php.ini の設定状況を確認し、register_globals の設定が有効になっていないかどうか確認してください。有効になっている場合、必要性の有無を確認し、不要であれば、無効にすることが暫定的な対策となります。
なお、PHP の設定において、register_globals は、PHP 4.2.0 より前のバージョンではデフォルトで有効になっています。（PHP 4.2.0 以降からはデフォルトで無効になっています）

【参考サイト】
XOOPS 2.3.2b - Security Release
http://www.xoops.org/modules/news/article.php?storyid=4563

【検証イメージ】



【検証ターゲットシステム】
XOOPS 2.3.1
PHP 5.2.6
CentOS 5

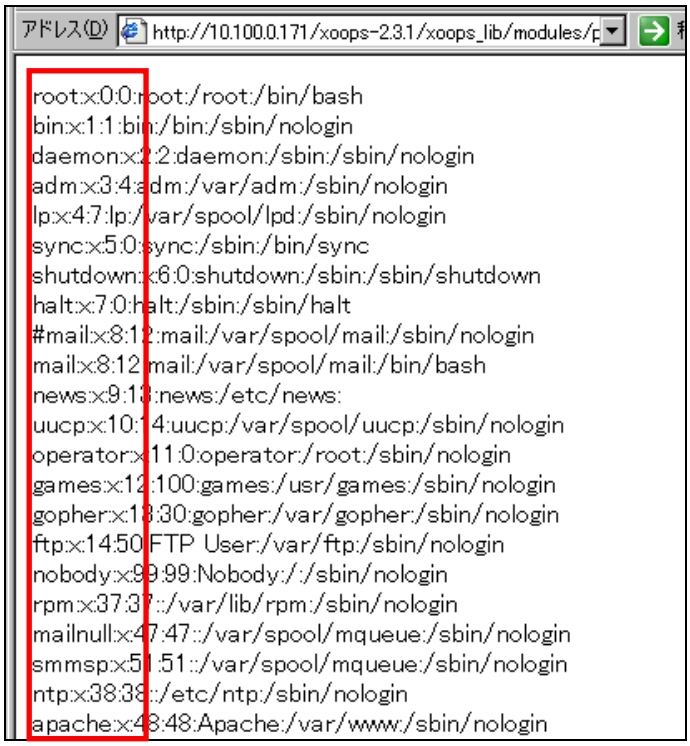
【検証概要】
ターゲットシステムに、細工した HTTP リクエストを送信することで、任意のファイルを読み出します。

NTTデータ・セキュリティ株式会社

【検証結果】

下図は、ディレクトリトラバーサルの脆弱性を利用し、ターゲットシステムのユーザ情報が格納されている「/etc/passwd」ファイルを、ブラウザから読み出した画面です。
赤枠（赤枠内の「：」（コロン）より前の部分）で示すとおり、ターゲットシステムに存在するユーザの一覧を取得できたと言えます。これにより、悪意のあるユーザに、SSH 等から当該ユーザに対するオンラインクラックを行われ、システムへの更なる制御の奪取を許す危険性があります。

ターゲットシステムの/etc/passwd を読み出した画面



【対策案】

最新バージョン（XOOPS 2.3.2b）へアップデートすることが推奨されます。
http://www.xoops.org/modules/news/article.php?storyid=4563

また、PHP の設定ファイル php.ini の設定状況を確認し、register_globals の設定が有効になっていないかどうか確認してください。有効になっている場合、必要性の有無を確認し、不要であれば、無効にすることが暫定的な対策となります。
なお、PHP の設定において、register_globals は、PHP 4.2.0 より前のバージョンではデフォルトで有効になっています。（PHP 4.2.0 以降からはデフォルトで無効になっています）

【参考サイト】

XOOPS 2.3.2b - Security Release
http://www.xoops.org/modules/news/article.php?storyid=4563

*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/