【Technical Report】
シグネチャリリース

2014 年 12 月 24 日
株式会社セキュアソフト

IE の整数オーバーフローの脆弱性を検知するシグネチャをリリース

本日、Internet Explorer の Integer Overflow 脆弱性や DDos 攻撃の不正コードを検知するシグネチャ等を含む、合計 4 件をリリースしました。

<シグネチャ名>

Microsoft Windows OLE Automation Array Remote Code Execution

<攻撃の説明>

この脆弱性は IE の VBScript エンジンが配列のサイズ変更を適切に処理できないため、任意のメモリ読み込み及び書き込みが可能になる脆弱性を悪用し、攻撃者は、Web ページにユーザのアクセスを誘導し攻撃を試みます。攻撃に成功すると、任意のコードを実行する事ができます。

参考 URL: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6332

<シグネチャ名>

Linux/DDoS.Lightaidra

<攻撃の説明>

Linux/DDoS.Lightaidra は、IRC 通信をベースにした不正コードです。
不正行為を行うため、IRC コマンドを受信し、脆弱な機器をスキャンし、直接に攻撃を行い、更に分散サービス攻撃系の不正行為を行い、botnet を確保します。

攻撃に成功すると、不正コードのダウンロードを試み、その不正コードを利用して分散サービス拒否の攻撃などを行います。

SecureSoft Sniper IPS をご利用のお客様は、自動アップデート、手動アップデートにより最新シグネチャを適用してご利用下さい。

以上