2016 年 8 月 23 日
株式会社セキュアソフト

脆弱性情報：HTTP_PROXY の脆弱性(CVE-2016-5385)

社内で稼働しているシステムは脆弱性がなく堅牢であることが理想的です。外部からの攻撃に対してはもちろんのこと内部からの攻撃に対しても堅牢であることが必要です。そうした中で日々多くのシステムの脆弱性が発見されています。特に Web サービス関連の脆弱性は多種多様で、XSS（クロスサイトスクリプティング）や DDoS 攻撃といった脅威が存在します。セキュリティ対策への関心が非常に高まっている中で、特に脆弱性対策は特に重要な対策であり、日々最新の情報を入手し継続的に行う必要があります。「Sniper シリーズ」は日々新たに発見される脆弱性に対して、セキュリティ脅威の動向を考慮しながらユーザーに適したシグネチャの配信を迅速に行っております。今回は HTTP_PROXY の脆弱性(CVE-2016-5385)について報告を致します。

HTTP_PROXY の脆弱性(CVE-2016-5385)はリモートから Proxy ヘッダを含むリクエストを受信した場合に、Web サーバの環境変数 HTTP_PROXY に意図しない値が設定され、脆弱性を悪用された場合、中間者攻撃が行われたり、不正なホスト（Web サイト）に接続させられたりするなどの可能性があります。弊社 IPS 製品 Sniper シリーズでは最新シグネチャを 8 月初旬に配信しました。配信したシグネチャの中で HTTP_PROXY の脆弱性(CVE-2016-5385)への対応が含まれています。

以下は、本脆弱性に関する詳細情報となります。

１．HTTP_PROXY の脆弱性(CVE-2016-5385)の対象システム

CGI または類似のコンテキストで動作している Web サーバ

２．HTTP_PROXY の脆弱性(CVE-2016-5385)の対処方法

① Web サービスで動作している製品のアップデートを行ってください。
② IPS 製品等でヘッダ Proxy が含まれるパケットを遮断してください。
（Sniper シリーズは最新シグネチャで対応済みです。）

3．HTTP_PROXY の脆弱性(CVE-2016-5385)に対する攻撃の一例：「不正サイトへの誘導」

① 不正な HTTP リクエスト
攻撃者が HTTP ヘッダ Proxy の値を”悪意あるプロキシサーバ”に細工してリクエストを A 社 Web サービスへ送信する。

② HTTP_PROXY 環境変数の書き換え
A 社 Web サーバは CGI の脆弱性により、HTTP_PROXY 環境変数の値を”悪意あるプロキシサーバ”に書き換える。

③ 一般の利用者が A 社 Web サービスへアクセス
一般の利用者が A 社 Web サービスを利用するために正常なリクエストを送信する。

④ 悪意あるプロキシサーバへリダイレクト
A 社 Web サービスが一般利用者のリクエストに対してプロキシサーバを経由させるために、HTTP_PROXY 環境変数に設定されている”悪意あるプロキシサーバ”にリダイレクトする。

⑤ 悪意あるプロキシサーバへの誘導
悪意あるプロキシサーバは A 社 Web サービスからのリダイレクトに対して、悪意ある Web サービス（サーバ）へ誘導する。

⑥ 情報漏洩、マルウェア感染等の被害が発生
一般の利用者は A 社 Web サービスを利用していると思っているが、意図せずに悪意ある Web サービス（サーバ）にアクセスすることで個人情報などの情報漏洩やマルウェア感染の被害が発生する。

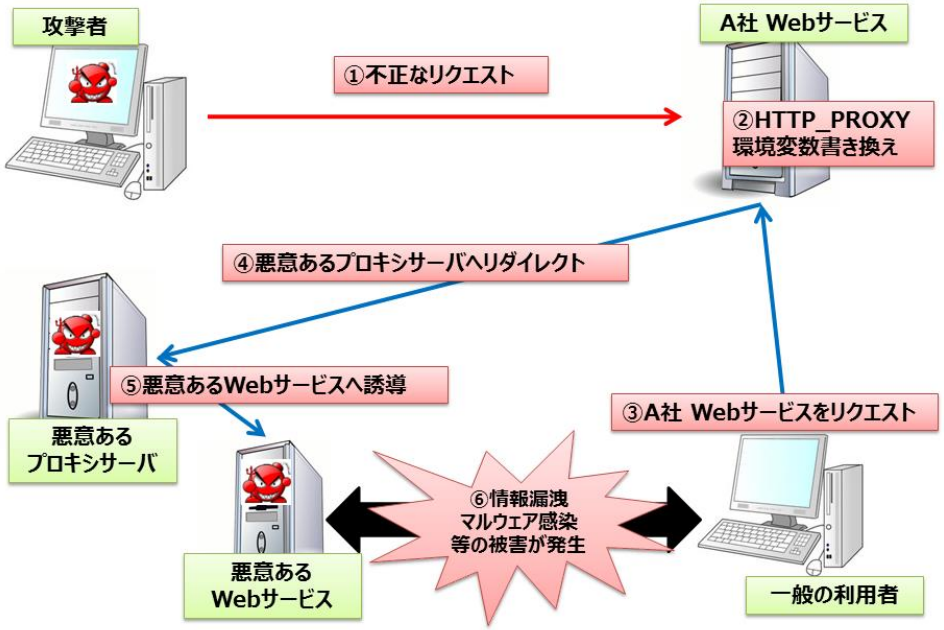

図 1 「不正サイトへの誘導」の概要

以上