



CYBSEC S.A.
www.cybsec.com

Advisory Name: httpprint Multiple Vulnerabilities

Vulnerability Class: Denial of Service, Arbitrary Script Injection

Release Date: 12/22/2005

Affected Applications:

- httpprint v202

Affected Platforms:

- Platform-Independent: Tested on Windows 2000 and Debian Linux

Local / Remote: Remote

Severity: Medium

Author: Mariano Nuñez Di Croce

Vendor Status:

- Confirmed, new version released.

Reference to Vulnerability Disclosure Policy:

http://www.cybsec.com/vulnerability_policy.pdf

Product Overview:

httpprint is a web server fingerprinting tool. It relies on web server characteristics to accurately identify web servers, despite the fact that they may have been obfuscated by changing the server banner strings, or by plug-ins such as mod_security or servermask.

Vulnerability Description:

1. Arbitrary Script Injection

A vulnerability exists in the way httpprint processes responses received from the host being scanned.

If the target host has modified the "Server" field of the HTTP Response headers, including DHTML code in it, it will be executed when the HTML output file is displayed by the browser.

© 2005 - CYBSEC S.A. Security Systems

It's important to emphasize that this code will be executed under "My Computer" Security Zone when viewed with IE.

Proof of Concept (using mod_security):

```
SecServerSignature "Microsoft-IIS/5.0<script>alert('test')</script>"
```

2. Denial of Service

If the server being fingerprinted is configured to reply with a "Server" field consisting of a string between 1030 and 1800 characters, httpprint fails to process the response properly, leading to an Access Violation condition, and ends abruptly.

This condition can be effectively used to develop a Denial of Service attack against the tool, preventing it from displaying the fingerprinting results.

Proof of Concept (using mod_security):

```
SecServerSignature "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA..."x1500
```

Mitigating Factors:

For the exploitation to succeed, httpprint must be used to analyze a web server specially configured to exploit the vulnerability.

Solutions:

Vendor has released httpprint v301, which fixes both vulnerabilities.

Vendor Response:

- 07/26/2005 - Vendor Notified about Script Injection vulnerability.
- 07/27/2005 - Vendor Confirmed Vulnerability.
- 09/01/2005 - Vendor Notified about DoS vulnerability.
- 09/27/2005 - Vendor Confirmed Vulnerability.
- 12/22/2005 - Vendor Releases New Version.
- 12/22/2005 - Vulnerability Public Disclosure.

Contact Information:

For more information regarding the vulnerability feel free to contact the author at [mnunez {at} cybsec.com](mailto:mnunez@cybsec.com).

For more information regarding CYBSEC: www.cybsec.com