



CYBSEC S.A.
www.cybsec.com

Advisory Name: Multiple Vendor Web Vulnerability Scanner Arbitrary Script Injection Vulnerability

Vulnerability Class: Script Injection

Release Date: 09.01.2005

Affected Applications:

- N-Stealth Commercial Edition < 5.8.0.38
- N-Stealth Free Edition < 5.8.1.03
- Nikto <= 1.35

Affected Platforms:

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

Local / Remote: Remote

Severity: Medium

Author: Mariano Nuñez Di Croce

Vendor Status: Confirmed. Update released.

Reference to Vulnerability Disclosure Policy:

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

Overview:

"N-Stealth is a vulnerability-assessment product that scans web servers to identify security problems and weaknesses that may allow an attacker to gain privileged access. The software comes with an extensive database of over 30,000 vulnerabilities and exploits".

"Nikto is an Open Source (GPL) web server scanner which performs comprehensive tests against web servers for multiple items, including over 3200 potentially dangerous files/CGIs, versions on over 625 servers, and version specific problems on over 230 servers".

Vulnerability Description:

A bug exists in the way multiple web vulnerability scanners process 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, this code will be executed by the browser when the HTML report is generated.

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>"
```

Besides, in N-Stealth main dialog, the Server header is displayed up to its 54th character. So, with the correct blank padding after the fake version banner, the DHTML code won't be noticed in this window.

Solutions:

N-Stealth vendor has released an update that fixes the vulnerability. Update can be downloaded at <http://www.nstalker.com>.

Nikto vendor has released an update that warns the user of dangers in viewing HTML reports. Update can be downloaded at <http://www.cirt.net>.

Vendor Response:

- 07.26.2005 - Vendors Notified.
- 07.26.2005 - Nikto Vendor Confirmed Vulnerability.
- 07.26.2005 - Nikto Vendor Supplied Update.
- 08.15.2005 - N-Stealth Vendor Confirmed Vulnerability.
- 08.25.2005 - N-Stealth Vendor Supplied Update.
- 09.01.2005 - Vulnerability Public Disclosure.

Special Thanks: Leandro Meiners.

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