

[NEWS] Multiple Vendor Web Vulnerability Scanner Arbitrary DHTML Injection

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-09/0013.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 09/05/05

To: list@securiteam.com

Date: 5 Sep 2005 13:46:46 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

Multiple Vendor Web Vulnerability Scanner Arbitrary DHTML Injection

SUMMARY

"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".

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.

Securiteam: [NEWS] Multiple Vendor Web Vulnerability Scanner Arbitrary DHTML Injection

DETAILS

Vulnerable Systems:

- * N-Stealth Commercial Edition version 5.8.0.37 and prior
- * N-Stealth Free Edition version 5.8.1.02 and prior
- * Nikto version 1.35 and prior

Immune Systems:

- * N-Stealth Commercial Edition version 5.8.0.38 or newer
- * N-Stealth Free Edition version 5.8.1.03 or newer
- * Nikto version 1.36 or newer

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>>
<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>>
<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

ADDITIONAL INFORMATION

The information has been provided by <<mailto:mnunez@cybsec.com>> Mariano Nu ez Di Croce.

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

Securiteam: [NEWS] Multiple Vendor Web Vulnerability Scanner Arbitrary DHTML Injection

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.