

[NT] Port80 Software ServerMask Inconsistencies

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-08/0035.html>

From: SecuriTeam (*support_at_securiteam.com*)

Date: 08/11/04

To: list@securiteam.com

Date: 11 Aug 2004 17:32:16 +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>

Port80 Software ServerMask Inconsistencies

SUMMARY

The <<http://www.port80software.com/products/servermask/>> ServerMask product is marketed as a solution for improving the security of Microsoft IIS servers by obfuscating header fields within HTTP responses:

"ServerMask 2.0 removes or modifies unnecessary response data. The software provides control over what Server header data, if any, is visible in HTTP responses."

In practice, ServerMask changes only a subset of the HTTP header fields, leaving a number of responses unmodified. These remaining headers still provide reliable clues to the server being Microsoft IIS.

The stated goal of the product, anonymization, is therefore not fully achieved as only a subset of identifying traits are obfuscated.

DETAILS

Analysis:

The ServerMask product is provided as an ISAPI filter for Microsoft IIS, and works by intercepting requests to the server and rewriting the HTTP header fields in responses.

Securiteam: [NT] Port80 Software ServerMask Inconsistencies

The product rewrites some server headers, removes some unnecessary ones, and reorders the remaining headers.

However, it leaves several obvious header fields unchanged that can be used to identify the server as Microsoft IIS, including:

- ETag:
- HTTP Status Message
- Allow: header in response to OPTIONS request

As it stands, the ServerMask product provides at best only an incomplete solution to anonymizing the server, whilst adding an additional product into the equation that must be maintained (and could potentially contain exploitable flaws).

Proof of concept:

To reproduce these issues, all that is required is access to a telnet client (or similar client providing equivalent functionality) and a suitable web server using the ServerMask product. For the purposes of this example Port80 Software's home site (www.port80software.com) is used.

Issue#1 – Standard IIS format ETag header

From a command prompt or shell, telnet, netc