

[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, netcat or other similar client should be used to connect to the web server on TCP port 80, e.g.

```
telnet www.port80software.com 80
```

The following extract should then be pasted into the session:

```
GET /images/H_horline.gif HTTP/1.1
Accept: */*
Connection: Keep-Alive
Host: www.port80software.com
```

The response received back should include:

```
HTTP/1.1 200 OK
Date: Mon, 24 Feb 2003 12:37:38 GMT
Server: Yes – We Use ServerMask
Last-Modified: Thu, 26 Sep 2002 00:07:29 GMT
ETag: "8e9dc0b3f064c21:9b0"
Accept-Ranges: bytes
Content-Length: 59
Content-Type: image/gif
```

The ETag header is the standard format returned by Microsoft IIS, and can be considered unique to that product.

Issue#2 – 404 Status Message Format

A session should again be initiated to the web port on the target, e.g.

```
telnet www.port80software.com 80
```

Securiteam: [NT] Port80 Software ServerMask Inconsistencies

The following request should then be used to attempt to retrieve a non-existent file from the server:

```
GET /not.there HTTP/1.1
Accept: */*
Connection: Keep-Alive
Host: www.port80software.com
```

The response should include headers similar to the following:

```
HTTP/1.1 404 Object Not Found
Date: Mon, 24 Feb 2003 12:49:54 GMT
Server: Yes - We Use ServerMask
Content-Length: 15383
Connection: close
Content-Type: text/html
```

The HTTP status message on the first line ("404 Object Not Found") is the standard format returned by Microsoft IIS, and differs from most other vendors.

Issue#3 – Standard IIS Format Allow header
A new session should be initiated to the web-server:

```
telnet www.port80software.com 80
```

An OPTIONS request should then be sent to solicit a server response:

```
OPTIONS /images/H_horline.gif HTTP/1.1
Accept: */*
Connection: Keep-Alive
Host: www.port80software.com
```

The headers should include the Allow response to the OPTIONS request:

```
HTTP/1.1 200 OK
Date: Mon, 24 Feb 2003 13:05:07 GMT
Server: Yes - We Use ServerMask
Content-Length: 0
Allow: OPTIONS, TRACE, GET, HEAD
```

The Allow header is the standard format, content and order returned by IIS.

Recommendations:

The ServerMask product should be revised and improved to provide full control over modifying the values of all header fields, to prevent such analysis revealing the nature of the underlying web-server.

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0105>>

Securiteam: [NT] Port80 Software ServerMask Inconsistencies

CAN-2003-0105

History:

Discovered: 20.02.03 (Martin O'Neal)

Vendor notified: 24.02.03

Document released: 10.08.04

The release process on this advisory has been drawn-out due to repeated requests from Port80, on the basis that a revised product that resolved the issues would be available shortly. However, after eighteen months of waiting (during which time Port80 has continued to actively sell the product) it has become clear that no such fix is imminent.

This advisory has been publicly released without a vendor fix being immediately available because the issues identified are not critical, and do not allow the host to be remotely compromised.

ADDITIONAL INFORMATION

The information has been provided by <mailto:jane.frankland@corsaire.com>

Jane Frankland.

The original article can be found at:

<<http://www.corsaire.com/advisories/c030224-001.txt>>

<http://www.corsaire.com/advisories/c030224-001.txt>

=====

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

=====

=====

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.