

RE: Possible IDS-evasion technique

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/vuln-dev/2002-02/0242.html>

From: Gary Golomb (gee_two@yahoo.com)

Date: 02/15/02

Date: Fri, 15 Feb 2002 12:54:50 -0800 (PST)

From: Gary Golomb <gee_two@yahoo.com>

To: vuln-dev@securityfocus.com

Hi there all...

Probably just problem with the way RealSecure is/was (I'm sure this doesn't happen in newer versions) looking for that particular string. I would imagine they are not making decisions based on user-supplied HTTP versions. (Then again, this is begins to tread on the 'ol debate of how protocol decoding should be used in ID. False Positives vs. False Negatives and the inverse relationship between reducing one and increasing the other...) Not the point of this thread or list though, so I'll shut-up there before the holy war freedom fighters get all excited...

Could the second two tests not trigger the same event the first two do (but still trigger a event that is not configured to send resets?). Just a thought - I'm not familiar with RealSecure...

Anyway, verified with Dragon:

```
[g@none]# nc 10.100.100.111 80
```

```
GET /cgi-bin/phf HTTP/0.9
```

```
HTTP/1.1 404 Not Found
```

```
Date: Fri, 15 Feb 2002 20:02:38 GMT
```

```
Server: Apache/1.3.19 (Unix) (Red-Hat/Linux) mod_ssl/2.8.1 OpenSSL/0.9.6 DAV/1.0.2 PHP/4.0.4p11
```

```
mod_perl/1.24_01
```

```
Connection: close
```

```
Content-Type: text/html; charset=iso-8859-1
```

and,

```
[g@none]# nc 10.100.100.111 80
```

```
GET /cgi-bin/phf HTTP/12.0
```

```
HTTP/1.1 400 Bad Request
```

```
Date: Fri, 15 Feb 2002 20:21:48 GMT
```

```
Server: Apache/1.3.19 (Unix) (Red-Hat/Linux) mod_ssl/2.8.1 OpenSSL/0.9.6 DAV/1.0.2 PHP/4.0.4p11
```

```
mod_perl/1.24_01
```

```
Connection: close
```

```
Transfer-Encoding: chunked
```

RE: Possible IDS-evasion technique

SecurityFocus Vuln-Dev: RE: Possible IDS-evasion technique

Content-Type: text/html; charset=iso-8859-1

[g@none]# /usr/dragon/tools/mklog -e WEB:CGI-PHF -l -f /usr/dragon/DB/2002Feb15/dragon.db

15:33:36 [T] x.x.x.x 10.100.100.111 [WEB:CGI-PHF] (tcp,dp=80,sp=32895) (test1-nids)

15:52:46 [T] x.x.x.x 10.100.100.111 [WEB:CGI-PHF] (tcp,dp=80,sp=32951) (test1-nids)

-----Original Message-----

From: Alla Bezroutchko

To: vuln-dev@securityfocus.com

Sent: 2/15/02 12:20 PM

Subject: Possible IDS-evasion technique

I've accidently found a way to bypass IDS detection for HTTP requests. I've seen this behaviour on some older version of IIS RealSecure network IDS and I wonder if this works on any other IDSes.

That particular IDS was set up to reset connections that match attack signatures, so I could see immediately if it was detected or not:

Request:

GET /cgi-bin/phf HTTP/1.0

Connection reset

Request:

GET /cgi-bin/phf

Connection reset

Request:

GET /cgi-bin/phf HTTP/1.2

Connection not reset, HTTP server replies "version not supported"

Request:

GET /cgi-bin/phf HTTP/0.9

Connection not reset, HTTP server replies "file not found"

Apparently the last form of request allows to get a meaningful reply from HTTP server while IDS does not mind it.

Apache and Netscape Entrprise will happily reply to the last form of request, didn't try it on other web servers.

Alla.

Do You Yahoo!?

Got something to say? Say it better with Yahoo! Video Mail

<http://mail.yahoo.com>

RE: Possible IDS-evasion technique

- *Previous message:* [Guilherme Mesquita: "Re: slocate bug."](#)
- *Maybe in reply to:* [Alla Bezroutchko: "Possible IDS-evasion technique"](#)
- *Next in thread:* [Sullo sq: "Re: Possible IDS-evasion technique"](#)
- *Messages sorted by:* [\[date \] \[thread \] \[subject \] \[author \] \[attachment \]](#)