

# [NEWS] Firewall Circumvention Possible with All Browsers

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-07/0131.html>

---

*From:* [support@securiteam.com](mailto:support@securiteam.com)

*Date:* 07/30/02

From: [support@securiteam.com](mailto:support@securiteam.com)

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: Tue, 30 Jul 2002 08:32:48 +0200 (CEST)

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

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> -- Know that you're safe.

-----

Firewall Circumvention Possible with All Browsers

---

## SUMMARY

The following exploit constitutes a security flaw in JavaScript's "Same Origin Policy" (SOP) [1]. Please note that this is *\*not\** the IE-specific flaw reported in February [2].

The exploit allows an attacker to use any JavaScript-enabled web browser behind a firewall to retrieve content from (HTTP GET) and interact with (HTTP <form/> POST) any HTTP server behind the firewall. If the client in use is Microsoft Internet Explorer 5.0+, Mozilla, or Netscape 6.2+, the attacker can also make calls to SOAP or XML-RPC web services deployed behind the firewall.

## DETAILS

### Status:

This advisory is being released in accordance with the Responsible Disclosure Draft RFC [3]. See the last section of this advisory for a timeline. Vendors were notified on 28-Jun-2002, 30 days prior to the public release.

## Securiteam: [NEWS] Firewall Circumvention Possible with All Browsers

As of 29-Jul-2002, \*no vendor\* has implemented a fix that will protect clients behind proxies (without external DNS) from the attack variant outlined in the section "Quick-Swap DNS".

Further vendor status can be found in the section "Vendor Responses".

Exploit:

1) Attacker controls DNS zone \*.baz.com, configuring it as follows:

- a) foo.bar.baz.com -> some web server operated by the attacker
- b) bar.baz.com -> 10.0.0.9 (some address behind BigCo's firewall)

2) The attacker induces unsuspecting user at BigCo to visit

<http://foo.bar.baz.com/>.

3) A JavaScript on said page sets document.domain to "baz.bar.com" (this is valid since baz.bar.com is a parent domain of foo.bar.baz.com). See [1]. Also, note that this step is not strictly necessary, but substantially improves the performance of the exploit and the ease of implementation.

4) JavaScript on the page then loads a page from

<http://bar.baz.com/somePrivatePage.html> into a hidden frame. This page will be retrieved from 10.0.0.9, a machine behind the firewall.

5) The JavaScript then extracts the contents of the other frame (it can do this since the two frames' document.domain matches), url-encodes it into a link and loads \*that\* link in another hidden frame, thereby transmitting the contents of the intranet page back to the attacker as part of the HTTP GET request. Large pages could use <form>s and an HTTP POST.

Moving beyond a single server:

By adding an entry X.Y.Z.baz.com for each address 10.X.Y.Z, this script could iteratively scan the entire 10.0.0.0/8 net block. A pop-under could be used to keep a window open (with the JavaScript probe running) long enough to get substantial coverage.

Attacking Web Services:

If the client in use is Microsoft Internet Explorer, this technique can be used to access arbitrary SOAP or XML-RPC based web services behind the firewall. Microsoft Internet Explorer 5.0 and later ship with an ActiveX control called "XMLHTTP", which allows JavaScripts to POST XML content to the server they originated from. Although XMLHTTP does not respect changes to document.domain, it is still vulnerable to this Quick-Swap DNS. Credit goes to Jared Smith-Mickelson for suggesting this possibility.

A similar attack should be feasible with Mozilla's XMLHttpRequest object [4].

Increased sophistication:

An even more sophisticated attack would involve the JavaScript querying the attacker's server for a list of IPs/URLs to fetch using this exploit.

## Securiteam: [NEWS] Firewall Circumvention Possible with All Browsers

If the attacker can induce enough users within BigCo to visit the malicious script (by spamming them?), the attacker could construct a proxy server that would route her requests to a cluster of slave JavaScripts. The attacker would effectively be able to open up a web browser and saunter around the company's intranet as if she were sitting right on it.

### Quick-Swap DNS:

This variation of the attack will still work even if browser vendors change their policy to prohibit changes to document.domain. In this situation, the attacker would need a DNS server with the refresh/expire TTL set to zero (no caching allowed). Once the user loads the page from the attacker's web server, the attacker would change her DNS records so that foo.bar.baz.com now points to 10.0.0.9. The exploit would proceed normally. A custom DNS server could be used to automate this process. By allocating a single hostname to each slave JavaScript, an arbitrary number of Clients can be modified to "lock in" the IP for a given hostname once a page is loaded, although this approach will fail for clients behind a proxy without DNS access.

### Short Term Solution:

Web servers behind firewalls should be configured to reject any HTTP requests with an unrecognized "Host" header, rather than serving pages from the "default" virtual host. This can be accomplished without patches by creating a "default" virtual host with no content, and creating a name-based virtual server for each hostname that the server is intended to serve as.

### Long Term Solution:

Many products have embedded HTTP servers that entirely ignore the Host header since they do not support name-based virtual hosts. The notion of a "default" virtual server is also very useful; it is doubtful that web server vendors will be willing to remove this feature simply to work around a flaw in popular web browsers.

Clearly, a long-term solution to this problem must involve a refinement of the SOP policy.

SOP should be enforced on an IP-by-IP basis, rather than a hostname-by-hostname basis, since the hostname-to-IP mapping is under the control of the attacker, while the IP-to-physical-server mapping is not.

Since some clients behind HTTP proxies do not have access to a DNS server that they can use for name-to-IP resolution, HTTP Proxies should return an additional header in the HTTP reply "Origin-Server-Address:", whose value is the network-layer address of the origin server. A web browser without DNS access that receives a script from a proxy that does not support this header must not be allowed to access content in any other frame, iframe, window, or layer.

### Short Term Workaround:

There is another tactic many enterprises can use to protect against this

## Securiteam: [NEWS] Firewall Circumvention Possible with All Browsers

in a simple, centralized manner. Any enterprise that forces its users' browsers to use a proxy server for "external" content may have an easy fix. Simply configure the proxy server to disallow any request whose Host is not the company's own domain \*and\* whose "remote" IP address is on the local network. E.G. in Squid ACL logic, something like

```
acl ToOurDomain dstdomain .example.com
acl ToOurLAN dst 10.0.0.0/8 192.168.0.0/16
http_access deny ToOurLAN !ToOurDomain
```

Since the victim.example.com user's browser will connect to the specified proxy server to get <http://bar.baz.com/somePrivatePage.html>, the proxy server can prevent the client attack without any hard-to-distribute client software updates.

More straightforward might be:

```
acl ToOurLAN dst 10.0.0.0/8 192.168.0.0/16
http_access deny ToOurLAN
```

Since in most cases the clients should never request an internal resource through the proxy server.

There's an assumption here, that the client software/browser will look at the URL's "hostname" component on its face ("bar.baz.com") instead of the IP address it represents ("10.0.0.9") when deciding if the URL represents a "local" resource (i.e., one to request via direct TCP) or a "remote" address that should go through the proxy server.

Of course enterprises that use have "straight" NAT are in trouble -- even places with transparent Web proxy servers would be out of luck, as the request for <http://bar.baz.com/somePrivatePage.html> is unlikely to hit the transparent proxy, as such networking magic is usually implemented on the egress point(s), not on multiple points inside the network. In a typical NAT setup, the request for <http://bar.baz.com/somePrivatePage.html> would go directly from desktop:someHighPort to target:80 & the device doing the transparent redirection would never see it happen.

Vendor Responses:

Netscape:

Netscape/Mozilla has included a patch in the CVS repository [5] that implements the following two refinements:

- 1) A change to document.domain is only honored if both the source and target frame altered document.domain.
- 2) If the client has access to external DNS, the hostname-to-IP mapping is "pinned" for the lifetime of the page.

These refinements defend against this vulnerability if the client has access to DNS. Clients behind proxies who lack DNS access are still vulnerable to the attack outlined in the section "Quick-Swap DNS".

## Securiteam: [NEWS] Firewall Circumvention Possible with All Browsers

### Microsoft:

Microsoft has investigated the issue discussed in the report, and agrees that the issue is bona fide from a technical standpoint. However, because of the difficulties associated with exploiting it (discussed below), Microsoft believes it is most appropriate to address the issue via a service pack. Accordingly, a fix has been included in IE 6 Service Pack 1, which is due to be released shortly.

Among the barriers that an attacker would face in attempting to exploit the vulnerability are the following:

- \* It could only be exploited if the user clicked a link within an email – it could not be exploited without user interaction.
- \* It would require that the attacker host a DNS server, a fact that would be traceable.
- \* The attacker would need detailed information about the internals of the user's network, such as intranet server names.
- \* If the intranet site were an HTTPS: site, a dialog would warn the user that the name on the site's certificate did not match the domain name.
- \* If the intranet site used cookie-based authentication, the attack would fail because the attacker's site would be unable to authenticate on behalf of the user
- \* The attack would not work against web servers configured to support multiple host headers, with the exception of any content served up at the "default" site.

### ADDITIONAL INFORMATION

#### References:

[1]

<<http://www.mozilla.org/projects/security/components/same-origin.html>>  
<http://www.mozilla.org/projects/security/components/same-origin.html> and  
<<http://developer.netscape.com/docs/manuals/communicator/jsguide4/sec.htm>>  
<http://developer.netscape.com/docs/manuals/communicator/jsguide4/sec.htm>

[2] <http://www.securiteam.com/windowsntfocus/6B00L003FU.html>

[3]

<<http://www.ietf.org/internet-drafts/draft-christey-wysopal-vuln-disclosure-00.txt>>  
<http://www.ietf.org/internet-drafts/draft-christey-wysopal-vuln-disclosure-00.txt>

[4]

<<http://unstable.elemental.com/mozilla/build/latest/mozilla/extensions/dox/interfacensIXMLHttpRequest.html>>  
<http://unstable.elemental.com/mozilla/build/latest/mozilla/extensions/dox/interfacensIXMLHttpRequest.html>

[5] <[http://bugzilla.mozilla.org/show\\_bug.cgi?id=154930](http://bugzilla.mozilla.org/show_bug.cgi?id=154930)>  
[http://bugzilla.mozilla.org/show\\_bug.cgi?id=154930](http://bugzilla.mozilla.org/show_bug.cgi?id=154930)

The information has been provided by <<mailto:adam@xwt.org>> Adam Megacz  
and <<mailto:peterw@usa.net>> Peter Watkins.

Securiteam: [NEWS] Firewall Circumvention Possible with All Browsers

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](mailto:list-unsubscribe@securiteam.com)

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

- 
- *Previous message:* [support@securiteam.com](mailto:support@securiteam.com): "[NEWS] Lucent Brick VPN Firewall Multiple Vulnerabilities"
  - *Messages sorted by:* [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)