

[Full-Disclosure] NAV 2003 vuln

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2003-10/1728.html>

From: GARCIA Lionel (SOGETI France EXPLOITATION SUD) (lionel.garcia_at_airbus.com)

Date: 10/29/03

To: full-disclosure@lists.netsys.com

Date: Wed, 29 Oct 2003 14:52:46 +0100

Hi there ! Source:

<http://www.digitalpranksters.com/advisories/symantec/InternetSec2003.html>

RISK: LOW

PRODUCT: Norton Internet Security 2003 v6.0.4.34 (Maybe others we only tested this version)

PRODUCT URL: http://www.symantec.com/sabu/nis/nis_pe/index.html

DP PUBLIC ADVISORY RELEASED: October 27, 2003

FOUND BY: KrazySnake - krazysnake@digitalpranksters.com

PROBLEM:

When Norton Internet Security 2003 blocks a web site, it returns a web page to the browser stating that the site has been blocked. This error message contains the URL which was requested. Norton Internet Security 2003 appears to do no validation or encoding of the URL before returning it in the error message. This allows an attacker to supply a URL that contains script. This script will run in the context of the blocked site.

We have marked this as a low risk because we believe in most situations, there will be little information of interest since the site is normally blocked (browser cookies from the blocked site probably do not exist, etc). However this does allow sites that are blocked to run script on the victim's machine when it shouldn't be allowed.

The HTML returned by Norton Internet Security 2003 when a site is blocked looks like the following:

```
<html><head><title>Site Blocked</title></head><body>
<br><b>Norton Internet Security has blocked access to this restricted
site.</b><br><hr><br>
<p><b>Site:
</b><b>If you think this web site is incorrectly categorized, visit the
Symantec <a
```

Full-Disclosure: [Full-Disclosure] NAV 2003 vuln

to report it.</p></body></html>

-

PROOF OF CONCEPT:

A URL like

[### RESOLUTION:](http://BlockedSite/page.cgi?>alert(document.domain)</SCRIPT> will run script.</u></p></div><div data-bbox=)

The fix is now available through the product's LiveUpdate functionality.

GREETINGS:

SkippyInside, AngryB, and Harmo.

Thanks to Symantec for fixing this issue.

DISCLAIMER:

Standard disclaimer applies. The opinions expressed in this advisory are our own and not of any company. The information within this advisory may change without notice. Use of this information constitutes acceptance for use in an AS IS condition. There are no warranties with regard to this information. In no event shall the author be liable for any damages whatsoever arising out of or in connection with the use or spread of this information. Any use of this information is at the user's own risk.

Full-Disclosure – We believe in it.

Charter: <http://lists.netsys.com/full-disclosure-charter.html>