

[GLSA 200802-08] Boost: Denial of Service

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2008-02/msg00236.html>

- *From:* Raphael Marichez <falco@xxxxxxxxxx>
 - *Date:* Thu, 14 Feb 2008 23:40:16 +0100
-

Gentoo Linux Security Advisory GLSA 200802-08

<http://security.gentoo.org/>

Severity: Normal
Title: Boost: Denial of Service
Date: February 14, 2008
Bugs: #205955
ID: 200802-08

Synopsis

=====

Two vulnerabilities have been reported in Boost, each one possibly resulting in a Denial of Service.

Background

=====

Boost is a set of C++ libraries, including the Boost.Regex library to process regular expressions.

Affected packages

=====

Package / Vulnerable / Unaffected

1 dev-libs/boost < 1.34.1-r2 >= 1.34.1-r2

Description

=====

Tavis Ormandy and Will Drewry from the Google Security Team reported a failed assertion in file `regex/v4/perl_matcher_non_recursive.hpp`

[GLSA 200802-08] Boost: Denial of Service

(CVE-2008-0171) and a NULL pointer dereference in function `get_repeat_type()` file `basic_regex_creator.hpp` (CVE-2008-0172) when processing regular expressions.

Impact

=====

A remote attacker could provide specially crafted regular expressions to an application using Boost, resulting in a crash.

Workaround

=====

There is no known workaround at this time.

Resolution

=====

All Boost users should upgrade to the latest version:

```
# emerge --sync
# emerge --ask --oneshot --verbose ">=dev-libs/boost-1.34.1-r2"
```

References

=====

[1] CVE-2008-0171

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0171>

[2] CVE-2008-0172

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0172>

Availability

=====

This GLSA and any updates to it are available for viewing at the Gentoo Security Website:

<http://security.gentoo.org/glsa/glsa-200802-08.xml>

Concerns?

=====

Security is a primary focus of Gentoo Linux and ensuring the confidentiality and security of our users machines is of utmost importance to us. Any security concerns should be addressed to security@xxxxxxxxxx or alternatively, you may file a bug at <http://bugs.gentoo.org>.

License

=====

Copyright 2008 Gentoo Foundation, Inc; referenced text belongs to its owner(s).

The contents of this document are licensed under the Creative Commons – Attribution / Share Alike license.

<http://creativecommons.org/licenses/by-sa/2.5>

Attachment: pgphED7 iQUOJP.pgp

Description: PGP signature