

[Full-Disclosure] ERRATA: [GLSA 200411-01] ppp: No denial of service vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2004-11/0102.html>

From: Luke Macken (lewk_at_gentoo.org)

Date: 11/02/04

To: gentoo-announce@gentoo.org

Date: Tue, 02 Nov 2004 16:02:49 -0500

Gentoo Linux Security Advisory GLSA 200411-01

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

Severity: Low

Title: ppp: No denial of service vulnerability

Date: November 01, 2004

Bugs: #69152

ID: 200411-01

Synopsis
=====

pppd contains a bug that allows an attacker to crash his own connection, but it cannot be used to deny service to other users.

Background
=====

ppp is a Unix implementation of the Point-to-Point Protocol.

Description
=====

The pppd server improperly verifies header fields, potentially leading to a crash of the pppd process handling the connection. However, since a separate pppd process handles each ppp connection, this would not affect any other connection, or prevent new connections from being established.

Impact

=====

We incorrectly thought that this bug could be exploited to deny service to all ppp users. It is not the case, this bug has no security impact whatsoever. Many thanks to Paul Mackerras from the Samba team for correcting our mistake.

Workaround

=====

There is no need for a workaround.

Resolution

=====

ppp users can keep their current versions.

References

=====

- [1] Incorrect BugTraq Advisory
<http://www.securityfocus.com/archive/1/379450>

Availability

=====

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

<http://security.gentoo.org/glsa/glsa-200411-01.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@gentoo.org or alternatively, you may file a bug at <http://bugs.gentoo.org>.

License

=====

Copyright 2004 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/1.0>

Full-Disclosure – We believe in it.

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

- application/pgp-signature attachment: This is a digitally signed message part