

[Full-disclosure] ERRATA: [GLSA 200505-13] FreeRADIUS: SQL injection and Denial of Service vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2005-05/0492.html>

From: Sune Kloppenborg Jeppesen (jaervosz_at_gentoo.org)

Date: 05/20/05

To: gentoo-announce@gentoo.org

Date: Fri, 20 May 2005 14:35:19 +0200

Gentoo Linux Security Advisory [ERRATA UPDATE] GLSA 200505-13:02

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

Severity: Normal

Title: FreeRADIUS: SQL injection and Denial of Service
vulnerability

Date: May 17, 2005

Updated: May 20, 2005

Bugs: #91736

ID: 200505-13:02

Errata

=====

This advisory incorrectly described FreeRADIUS versions as being vulnerable to a remote compromise. After further verifications, it appears to only result in potential Denial of Service. The SQL injection issue is not affected by this. Many thanks to Nicolas Baradakis for bringing this to our attention.

The corrected sections appear below.

Synopsis

=====

The FreeRADIUS server is vulnerable to an SQL injection attack and a

buffer overflow, possibly resulting in disclosure and modification of data and Denial of Service.

Affected packages

=====

Package / Vulnerable / Unaffected

1 net-dialup/freeradius < 1.0.2-r4 >= 1.0.2-r4

Description

=====

Primoz Bratanic discovered that the `sql_escape_func` function of FreeRADIUS may be vulnerable to a buffer overflow (BID 13541). He also discovered that FreeRADIUS fails to sanitize user-input before using it in a SQL query, possibly allowing SQL command injection (BID 13540).

Impact

=====

By supplying carefully crafted input, a malicious user could cause an SQL injection or a buffer overflow, possibly leading to the disclosure and the modification of sensitive data or Denial of Service by crashing the server.

Resolution

=====

All FreeRADIUS users should upgrade to the latest available version:

```
# emerge --sync
# emerge --ask --oneshot --verbose ">=net-dialup/freeradius-1.0.2-r4"
```

Availability

=====

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

<http://security.gentoo.org/glsa/glsa-200505-13.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 2005 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/2.0>

Full-Disclosure – We believe in it.

Charter: <http://lists.grok.org.uk/full-disclosure-charter.html>

Hosted and sponsored by Secunia – <http://secunia.com/>

- application/pgp-signature attachment: [stored](#)