

[Full-disclosure] [GLSA 200508-21] phpWebSite: Arbitrary command execution through XML-RPC and SQL injection

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2005-08/1069.html>

From: Sune Kloppenborg Jeppesen (jaervosz_at_gentoo.org)

Date: 08/31/05

To: gentoo-announce@gentoo.org

Date: Wed, 31 Aug 2005 16:32:09 +0200

Gentoo Linux Security Advisory GLSA 200508-21

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

Severity: High

Title: phpWebSite: Arbitrary command execution through XML-RPC and
SQL injection

Date: August 31, 2005

Bugs: #102785

ID: 200508-21

Synopsis
=====

phpWebSite is vulnerable to multiple issues which result in the execution of arbitrary code and SQL injection.

Background
=====

phpWebSite is a web site content management system.

Affected packages
=====

Package / Vulnerable / Unaffected

1 www-apps/phpwebsite < 0.10.2_rc2 >= 0.10.2_rc2

Description

=====

phpWebSite uses an XML-RPC library that improperly handles XML-RPC requests and responses with malformed nested tags. Furthermore, "matrix_killer" reported that phpWebSite is vulnerable to an SQL injection attack.

Impact

=====

A malicious remote user could exploit this vulnerability to inject arbitrary PHP script code into eval() statements by sending a specially crafted XML document, and also inject SQL commands to access the underlying database directly.

Workaround

=====

There is no known workaround at this time.

Resolution

=====

All phpWebSite users should upgrade to the latest version:

```
# emerge --sync
# emerge --ask --oneshot --verbose ">=www-apps/phpwebsite-0.10.2_rc2"
```

References

=====

- [1] CAN-2005-2498
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2498>
- [2] Original Advisory
<http://archives.neohapsis.com/archives/fulldisclosure/2005-08/0497.html>

Availability

=====

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

<http://security.gentoo.org/glsa/glsa-200508-21.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](#)