

[Full-Disclosure] [gentoo-announce] [GLSA 200503-06] BidWatcher: Format string vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2005-03/0139.html>

From: Sune Kloppenborg Jeppesen (jaervosz_at_gentoo.org)

Date: 03/03/05

Date: Thu, 3 Mar 2005 22:27:57 +0100

To: the_eye@drei.at

Gentoo Linux Security Advisory GLSA 200503-06

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

Severity: Normal

Title: BidWatcher: Format string vulnerability

Date: March 03, 2005

Bugs: #82460

ID: 200503-06

Synopsis
=====

BidWatcher is vulnerable to a format string vulnerability, potentially allowing arbitrary code execution.

Background
=====

BidWatcher is a free auction tool for eBay users to keep track of their auctions.

Affected packages
=====

Package / Vulnerable / Unaffected

1 net-misc/bidwatcher < 1.3.17 >= 1.3.17

Description

=====

Ulf Harnhammar discovered a format string vulnerability in "netstuff.cpp".

Impact

=====

Remote attackers can potentially exploit this vulnerability by sending specially crafted responses via an eBay HTTP server or a man-in-the-middle attack to execute arbitrary malicious code.

Workaround

=====

There is no known workaround at this time.

Resolution

=====

All BidWatcher users should upgrade to the latest version:

```
# emerge --sync
# emerge --ask --oneshot --verbose ">=net-misc/bidwatcher-1.13.17"
```

References

=====

[1] CAN-2005-0158
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0158>

Availability

=====

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

<http://security.gentoo.org/glsa/glsa-200503-06.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.netsys.com/full-disclosure-charter.html>

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