

[Full-Disclosure] [gentoo-announce] [GLSA 200501-16] Konqueror: Java sandbox vulnerabilities

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2005-01/0370.html>

From: Sune Kloppenborg Jeppesen (jaervosz_at_gentoo.org)

Date: 01/11/05

Date: Tue, 11 Jan 2005 14:06:17 +0100

To: the_eye@drei.at

Gentoo Linux Security Advisory GLSA 200501-16

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

Severity: Normal

Title: Konqueror: Java sandbox vulnerabilities

Date: January 11, 2005

Bugs: #72750

ID: 200501-16

Synopsis

=====

The Java sandbox environment in Konqueror can be bypassed to access arbitrary packages, allowing untrusted Java applets to perform unrestricted actions on the host system.

Background

=====

KDE is a feature-rich graphical desktop environment for Linux and Unix-like Operating Systems. Konqueror is the KDE web browser and file manager.

Affected packages

=====

Package / Vulnerable / Unaffected

1 kde-base/kdelibs < 3.3.2 >= 3.3.2

Description

=====

Konqueror contains two errors that allow JavaScript scripts and Java applets to have access to restricted Java classes.

Impact

=====

A remote attacker could embed a malicious Java applet in a web page and entice a victim to view it. This applet can then bypass security restrictions and execute any command, or access any file with the rights of the user running Konqueror.

Workaround

=====

There is no known workaround at this time.

Resolution

=====

All kdelibs users should upgrade to the latest version:

```
# emerge --sync  
# emerge --ask --oneshot --verbose kde-base/kdelibs
```

Note: There is currently no fixed stable version for sparc.

References

=====

- [1] KDE Security Advisory: Konqueror Java Vulnerability
<http://www.kde.org/info/security/advisory-20041220-1.txt>
- [2] CAN 2004-1145
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1145>

Availability

=====

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

<http://security.gentoo.org/glsa/glsa-200501-16.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](#)