

[GLSA 200805-03] Multiple X11 terminals: Local privilege escalation

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2008-05/msg00086.html>

- *From:* Tobias Heinlein <keytoaster@xxxxxxxxxx>
 - *Date:* Wed, 07 May 2008 20:56:39 +0200
-

Gentoo Linux Security Advisory GLSA 200805-03

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

Severity: Normal

Title: Multiple X11 terminals: Local privilege escalation

Date: May 07, 2008

Bugs: #216833, #217819, #219746, #219750, #219754, #219760, #219762

ID: 200805-03

Synopsis

=====

A vulnerability was found in aterm, Eterm, Mrxvt, multi-aterm, RXVT, rxvt-unicode, and wterm, allowing for local privilege escalation.

Background

=====

Aterm, Eterm, Mrxvt, multi-aterm, RXVT, rxvt-unicode, and wterm are X11 terminal emulators.

Affected packages

=====

Package / Vulnerable / Unaffected

1 x11-terms/aterm < 1.0.1-r1 >= 1.0.1-r1
2 x11-terms/eterm < 0.9.4-r1 >= 0.9.4-r1
3 x11-terms/mrxvt < 0.5.3-r2 >= 0.5.3-r2
4 x11-terms/multi-aterm < 0.2.1-r1 >= 0.2.1-r1
5 x11-terms/rxvt < 2.7.10-r4 >= 2.7.10-r4
6 x11-terms/rxvt-unicode < 9.02-r1 >= 9.02-r1

7 x11-terms/wterm < 6.2.9-r3 >= 6.2.9-r3

7 affected packages on all of their supported architectures.

Description

=====

Bernhard R. Link discovered that Eterm opens a terminal on :0 if the "--display" option is not specified and the DISPLAY environment variable is not set. Further research by the Gentoo Security Team has shown that aterm, Mrxvt, multi-aterm, RXVT, rxvt-unicode, and wterm are also affected.

Impact

=====

A local attacker could exploit this vulnerability to hijack X11 terminals of other users.

Workaround

=====

There is no known workaround at this time.

Resolution

=====

All aterm users should upgrade to the latest version:

```
# emerge --sync
# emerge --ask --oneshot --verbose ">=x11-terms/aterm-1.0.1-r1"
```

All Eterm users should upgrade to the latest version:

```
# emerge --sync
# emerge --ask --oneshot --verbose ">=x11-terms/eterm-0.9.4-r1"
```

All Mrxvt users should upgrade to the latest version:

```
# emerge --sync
# emerge --ask --oneshot --verbose ">=x11-terms/mrxvt-0.5.3-r2"
```

All multi-aterm users should upgrade to the latest version:

```
# emerge --sync
# emerge --ask --oneshot --verbose ">=x11-terms/multi-aterm-0.2.1-r1"
```

All RXVT users should upgrade to the latest version:

```
# emerge --sync
```

[GLSA 200805-03] Multiple X11 terminals: Local privilege escalation

```
# emerge --ask --oneshot --verbose ">=x11-terms/rxvt-2.7.10-r4"
```

All rxvt-unicode users should upgrade to the latest version:

```
# emerge --sync
```

```
# emerge --ask --oneshot --verbose ">=x11-terms/rxvt-unicode-9.02-r1"
```

All wterm users should upgrade to the latest version:

```
# emerge --sync
```

```
# emerge --ask --oneshot --verbose ">=x11-terms/wterm-6.2.9-r3"
```

References

=====

[1] CVE-2008-1142

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1142>

[2] CVE-2008-1692

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1692>

Availability

=====

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

<http://security.gentoo.org/glsa/glsa-200805-03.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@xxxxxxxxxx or alternatively, you may file a bug at <http://bugs.gentoo.org>.

License

=====

Copyright 2008 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/2.5>

Attachment: *signature.asc*

Description: OpenPGP digital signature