

[GLSA 200707-10] Festival: Privilege elevation

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2007-07/msg00298.html>

- *From:* Raphael Marichez <falco@xxxxxxxxxxx>
 - *Date:* Wed, 25 Jul 2007 23:30:54 +0200
-

Gentoo Linux Security Advisory GLSA 200707-10

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

Severity: High
Title: Festival: Privilege elevation
Date: July 25, 2007
Bugs: #170477
ID: 200707-10

Synopsis

=====

A vulnerability has been discovered in Festival, allowing for a local privilege escalation.

Background

=====

Festival is a text-to-speech accessibility program.

Affected packages

=====

Package / Vulnerable / Unaffected

1 app-accessibility/festival < 1.95_beta-r4 >= 1.95_beta-r4

Description

=====

Konstantine Shirow reported a vulnerability in default Gentoo configurations of Festival. The daemon is configured to run with root privileges and to listen on localhost, without requiring a password.

Impact

=====

A local attacker could gain root privileges by connecting to the daemon and execute arbitrary commands.

Workaround

=====

Set a password in the configuration file `/etc/festival/server.scm` by adding the line: `(set! server_passwd password)`

Resolution

=====

All Festival users should upgrade to the latest version:

```
# emerge --sync
# emerge --ask --oneshot --verbose ">=app-accessibility/festival-1.95_beta-r4"
```

Availability

=====

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

<http://security.gentoo.org/glsa/glsa-200707-10.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 2007 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: [pgp75Siwtcahc.pgp](#)

Description: PGP signature