

[Full-Disclosure] [gentoo-announce] [GLSA 200405-09] ProFTPD Access Control List bypass vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2004-05/1078.html>

From: Kurt Lieber (klieber_at_gentoo.org)

Date: 05/19/04

Date: Wed, 19 May 2004 08:03:40 -0400

To: gentoo-announce@lists.gentoo.org

Gentoo Linux Security Advisory GLSA 200405-09

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

Severity: High

Title: ProFTPD Access Control List bypass vulnerability

Date: May 19, 2004

Bugs: #49496

ID: 200405-09

Synopsis

=====

Version 1.2.9 of ProFTPD introduced a vulnerability that causes CIDR-based Access Control Lists (ACLs) to be treated as "AllowAll", thereby allowing remote users full access to files available to the FTP daemon.

Background

=====

ProFTPD is an FTP daemon.

Affected packages

=====

Package / Vulnerable / Unaffected

1 net-ftp/proftpd == 1.2.9-r1 >= 1.2.9-r2
1 net-ftp/proftpd == 1.2.9 >= 1.2.9-r2

Description

=====

ProFTPD 1.2.9 introduced a vulnerability that allows CIDR-based ACLs (such as 10.0.0.1/24) to be bypassed. The CIDR ACLs are disregarded, with the net effect being similar to an "AllowAll" directive.

Impact

=====

This vulnerability may allow unauthorized files, including critical system files to be downloaded and/or modified, thereby allowing a potential remote compromise of the server.

Workaround

=====

Users may work around the problem by avoiding use of CIDR-based ACLs.

Resolution

=====

ProFTPD users are encouraged to upgrade to the latest version of the package:

```
# emerge sync  
  
# emerge -pv ">=net-ftp/proftpd-1.2.9-r2"  
# emerge ">=net-ftp/proftpd-1.2.9-r2"
```

References

=====

[1] CAN-2004-0432
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0432>

Availability

=====

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

<http://security.gentoo.org/glsa/glsa-200405-09.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 2004 Gentoo Technologies, 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/1.0>

Full-Disclosure – We believe in it.

Charter: <http://lists.netsys.com/full-disclosure-charter.html>

- application/pgp-signature attachment: stored