PHP Buffer Overflow in Wordwrap() Function May Let Remote Users Crash the Server - Security

NEWS_PDF_AUTHOR: w4z004

NEWS_PDF_DATE: 2002/12/31 9:41:00

in: http://www.securitytracker.com/alerts/2002/Dec/1005863.html

SecurityTracker Alert ID: 1005863
CVE Reference: GENERIC-MAP-NOMATCH (Links to External Site)
Date: Dec 27 2002

Impact: Denial of service via network, Execution of arbitrary code via network, User access via network

Fix Available: Yes Vendor Confirmed: Yes

Version(s): after 4.1.2 and before 4.3.0

Description: A buffer overflow vulnerability was reported in PHP. A remote user could cause the web service to crash or possibly execute arbitrary code.

It is reported that a remote user can supply specially crafted input to an application that uses the wordwrap() function to trigger the overflow and overwrite the heap. According to the report, executing arbitrary code may be difficult, but possible. Impact: A remote user can cause the web service to crash. A remote user may potentially be able to execute arbitrary code on the system. Solution: The vendor has released a fixed version (4.3.0), available at: http://www.php.net/downloads.php Vendor URL: bugs.php.net/bug.php?id=20927 (Links to External Site) Cause: Boundary error Underlying OS: Linux (Any), UNIX (Any), Windows (Any) Reported By: "David F. Skoll" Message History: None.
---------- Source Message Contents ---------- Date: Fri, 27 Dec 2002 16:43:44 -0500 (EST) From: "David F. Skoll" Subject: Buffer overflow in PHP "wordwrap" function -----BEGIN PGP SIGNED MESSAGE----- Hash: SHA1 There is a buffer overflow in PHP's built-in "wordwrap" function for PHP versions greater than 4.1.2 and less than 4.3.0. Please see http://bugs.php.net/bug.php?id=20927 for details. If you use the wordwrap() function on user-supplied input, a specially-crafted input can overflow the allocated buffer and overwrite the heap. Exploit looks very difficult, but still theoretically possible. Status: Bug cause discovered: 10 Dec 2002 PHP team notified: 10 Dec 2002 Bug fixed in CVS: 12 Dec 2002 PHP 4.3.0 released: 27 Dec 2002 Kudos to the PHP team for their extremely rapid reaction. Recommendations: Don't upgrade from 4.1.2 if you are certain there are no security problems

with your 4.1.2 setup and you may be vulnerable to the wordwrap() bug. Otherwise, upgrade to 4.3.0 - -- David F. Skoll Roaring Penguin Software Inc. | http://www.roaringpenguin.com GPG fingerprint: 58BB 6D86 6F6F 84D0 2C89 59D1 CD1C CAEE 1362 4131 GPG public key: http://www.roaringpenguin.com/dskoll-key-2003.txt ID: 13624131 -----BEGIN PGP SIGNATURE----- Version: GnuPG v1.0.6 (GNU/Linux) Comment: For info see http://quantumlab.net/pine_privacy_guard/ iD8DBQE+DMmUzRzK7hNiQTERAngfAKCAz0vUMBS4o+ZMLExpE6Q+ABcKdgCdHVpD 24SOO2IcJ1VPotswMfOQa58= =DX/n -----END PGP SIGNATURE-----

in: http://www.securitytracker.com/alerts/2002/Dec/1005863.html

SecurityTracker Alert ID: 1005863
CVE Reference: GENERIC-MAP-NOMATCH (Links to External Site)
Date: Dec 27 2002

Impact: Denial of service via network, Execution of arbitrary code via network, User access via network

Fix Available: Yes Vendor Confirmed: Yes

Version(s): after 4.1.2 and before 4.3.0

Description: A buffer overflow vulnerability was reported in PHP. A remote user could cause the web service to crash or possibly execute arbitrary code.

It is reported that a remote user can supply specially crafted input to an application that uses the wordwrap() function to trigger the overflow and overwrite the heap. According to the report, executing arbitrary code may be difficult, but possible. Impact: A remote user can cause the web service to crash. A remote user may potentially be able to execute arbitrary code on the system. Solution: The vendor has released a fixed version (4.3.0), available at: http://www.php.net/downloads.php Vendor URL: bugs.php.net/bug.php?id=20927 (Links to External Site) Cause: Boundary error Underlying OS: Linux (Any), UNIX (Any), Windows (Any) Reported By: "David F. Skoll" Message History: None.
---------- Source Message Contents ---------- Date: Fri, 27 Dec 2002 16:43:44 -0500 (EST) From: "David F. Skoll" Subject: Buffer overflow in PHP "wordwrap" function -----BEGIN PGP SIGNED MESSAGE----- Hash: SHA1 There is a buffer overflow in PHP's built-in "wordwrap" function for PHP versions greater than 4.1.2 and less than 4.3.0. Please see http://bugs.php.net/bug.php?id=20927 for details. If you use the wordwrap() function on user-supplied input, a specially-crafted input can overflow the allocated buffer and overwrite the heap. Exploit looks very difficult, but still theoretically possible. Status: Bug cause discovered: 10 Dec 2002 PHP team notified: 10 Dec 2002 Bug fixed in CVS: 12 Dec 2002 PHP 4.3.0 released: 27 Dec 2002 Kudos to the PHP team for their extremely rapid reaction. Recommendations: Don't upgrade from 4.1.2 if you are certain there are no security problems with your 4.1.2 setup and you may be vulnerable to the wordwrap() bug. Otherwise, upgrade to 4.3.0 - -- David F. Skoll Roaring Penguin Software Inc. | http://www.roaringpenguin.com GPG fingerprint: 58BB 6D86 6F6F 84D0 2C89 59D1 CD1C CAEE 1362 4131 GPG public key: http://www.roaringpenguin.com/dskoll-key-2003.txt ID: 13624131 -----BEGIN PGP SIGNATURE----- Version: GnuPG v1.0.6 (GNU/Linux) Comment: For info see http://quantumlab.net/pine_privacy_guard/
iD8DBQE+DMmUzRzK7hNiQTERAngfAKCAz0vUMBS4o+ZMLExpE6Q+ABcKdgCdHVpD 24SOO2IcJ1VPotswMfOQa58= =DX/n -----END PGP SIGNATURE-----