

# CERT Advisory CA-2002-21 Vulnerability in PHP

*Source:* <http://www.derkeiler.com/Mailing-Lists/Cert/2002-07/0004.html>

---

*From:* CERT Advisory ([cert-advisory@cert.org](mailto:cert-advisory@cert.org))

*Date:* 07/23/02

Date: Mon, 22 Jul 2002 19:09:01 -0400 (EDT)  
From: CERT Advisory <[cert-advisory@cert.org](mailto:cert-advisory@cert.org)>  
To: [cert-advisory@cert.org](mailto:cert-advisory@cert.org)

-----BEGIN PGP SIGNED MESSAGE-----

CERT Advisory CA-2002-21 Vulnerability in PHP

Original release date: July 22, 2002

Last revised: ---

Source: CERT/CC

A complete revision history can be found at the end of this file.

## Systems Affected

- \* Systems running PHP versions 4.2.0 or 4.2.1

## Overview

A vulnerability has been discovered in PHP. This vulnerability could be used by a remote attacker to execute arbitrary code or crash PHP and/or the web server.

## I. Description

PHP is a popular scripting language in widespread use. For more information about PHP, see

<http://www.php.net/manual/en/faq.general.php>

The vulnerability occurs in the portion of PHP code responsible for handling file uploads, specifically multipart/form-data. By sending a specially crafted POST request to the web server, an attacker can corrupt the internal data structures used by PHP. Specifically, an intruder can cause an improperly initialized memory structure to be freed. In most cases, an intruder can use this flaw to crash PHP or the web server. Under some circumstances, an intruder may be able to take advantage of this flaw to execute arbitrary code with the privileges of the web server.

## Cert: CERT Advisory CA-2002-21 Vulnerability in PHP

You may be aware that freeing memory at inappropriate times in some implementations of malloc and free does not usually result in the execution of arbitrary code. However, because PHP utilizes its own memory management system, the implementation of malloc and free is irrelevant to this problem.

Stefan Esser of e-matters GmbH has indicated that intruders cannot execute code on x86 systems. However, we encourage system administrators to apply patches on x86 systems as well to guard against denial-of-service attacks and as-yet-unknown attack techniques that may permit the execution of code on x86 architectures.

This vulnerability was discovered by e-matters GmbH and is described in detail in their advisory. The PHP Group has also issued an advisory. A list of vendors contacted by the CERT/CC and their status regarding this vulnerability is available in VU#929115.

Although this vulnerability only affects PHP 4.2.0 and 4.2.1, e-matters GmbH has previously identified vulnerabilities in older versions of PHP. If you are running older versions of PHP, we encourage you to review <http://security.e-matters.de/advisories/012002.html>

### II. Impact

A remote attacker can execute arbitrary code on a vulnerable system. An attacker may not be able to execute code on x86 architectures due to the way the stack is structured. However, an attacker can leverage this vulnerability to crash PHP and/or the web server running on an x86 architecture.

### III. Solution

Apply a patch from your vendor

Appendix A contains information provided by vendors for this advisory. As vendors report new information to the CERT/CC, we will update this section and note the changes in our revision history. If a particular vendor is not listed below, we have not received their comments. Please contact your vendor directly.

Upgrade to the latest version of PHP

If a patch is not available from your vendor, upgrade to version 4.2.2.

Deny POST requests

Until patches or an update can be applied, you may wish to deny POST requests. The following workaround is taken from the PHP Security Advisory:

## Cert: CERT Advisory CA-2002-21 Vulnerability in PHP

If the PHP applications on an affected web server do not rely on HTTP POST input from user agents, it is often possible to deny POST requests on the web server.

In the Apache web server, for example, this is possible with the following code included in the main configuration file or a top-level .htaccess file:

```
<Limit POST>  
  Order deny,allow  
  Deny from all  
</Limit>
```

Note that an existing configuration and/or .htaccess file may have parameters contradicting the example given above.

### Disable vulnerable service

Until you can upgrade or apply patches, you may wish to disable PHP. As a best practice, the CERT/CC recommends disabling all services that are not explicitly required. Before deciding to disable PHP, carefully consider your service requirements.

### Appendix A. – Vendor Information

This appendix contains information provided by vendors for this advisory. As vendors report new information to the CERT/CC, we will update this section and note the changes in our revision history. If a particular vendor is not listed below, we have not received their comments.

#### Apple Computer Inc.

Mac OS X and Mac OS X Server are shipping with PHP version 4.1.2 which does not contain the vulnerability described in this alert.

#### Caldera

Caldera OpenLinux does not provide either vulnerable version (4.2.0, 4.2.1) of PHP in their products. Therefore, Caldera products are not vulnerable to this issue.

#### Compaq Computer Corporation

SOURCE: Compaq Computer Corporation, a wholly-owned subsidiary of Hewlett-Packard Company and Hewlett-Packard Company HP Services Software Security Response Team  
x-ref: SSRT2300 php post requests  
At the time of writing this document, Compaq is currently investigating the potential impact to Compaq's released

## Cert: CERT Advisory CA-2002-21 Vulnerability in PHP

Operating System software products.

As further information becomes available Compaq will provide notice of the availability of any necessary patches through standard security bulletin announcements and be available from your normal HP Services supportchannel.

### Cray Inc.

Cray, Inc. does not supply PHP on any of its systems.

### Debian

Debian GNU/Linux stable aka 3.0 is not vulnerable.

Debian GNU/Linux testing is not vulnerable.

Debian GNU/Linux unstable is vulnerable.

The problem effects PHP versions 4.2.0 and 4.2.1. Woody ships an older version of PHP (4.1.2), that doesn't contain the vulnerable function.

### FreeBSD

FreeBSD does not include any version of PHP by default, and so is not vulnerable; however, the FreeBSD Ports Collection does contain the PHP4 package. Updates to the PHP4 package are in progress and a corrected package will be available in the near future.

### Guardian Digital

Guardian Digital has not shipped PHP 4.2.x in any versions of EnGarde, therefore we are not believed to be vulnerable at this time.

### Hewlett-Packard Company

SOURCE: Hewlett-Packard Company Security Response Team  
At the time of writing this document, Hewlett Packard is currently investigating the potential impact to HP's released Operating System software products.

As further information becomes available HP will provide notice of the availability of any necessary patches through standard security bulletin announcements and be available from your normal HP Services support channel.

### IBM

IBM is not vulnerable to the above vulnerabilities in PHP. We do supply the PHP packages for AIX through the AIX Toolbox for Linux Applications. However, these packages are at 4.0.6 and also incorporate the security patch from 2/27/2002.

## Cert: CERT Advisory CA-2002-21 Vulnerability in PHP

### Mandrakesoft

Mandrake Linux does not ship with PHP version 4.2.x and as such is not vulnerable. The Mandrake Linux cooker does currently contain PHP 4.2.1 and will be updated shortly, but cooker should not be used in a production environment and no advisory will be issued.

### Microsoft Corporation

Microsoft products are not affected by the issues detailed in this advisory.

### Network Appliance

No Netapp products are vulnerable to this.

### Red Hat Inc.

None of our commercial releases ship with vulnerable versions of PHP (4.2.0, 4.2.1).

### SuSE Inc.

SuSE Linux is not vulnerable to this problem, as we do not ship PHP 4.2.x.

---

The CERT/CC acknowledges e-matters GmbH for discovering and reporting this vulnerability.

---

Author: Ian A. Finlay.

---

This document is available from:  
<http://www.cert.org/advisories/CA-2002-21.html>

---

### CERT/CC Contact Information

Email: [cert@cert.org](mailto:cert@cert.org)

Phone: +1 412-268-7090 (24-hour hotline)

Fax: +1 412-268-6989

Postal address:

CERT Coordination Center  
Software Engineering Institute  
Carnegie Mellon University  
Pittsburgh PA 15213-3890  
U.S.A.

## Cert: CERT Advisory CA-2002-21 Vulnerability in PHP

CERT/CC personnel answer the hotline 08:00-17:00 EST(GMT-5) / EDT(GMT-4) Monday through Friday; they are on call for emergencies during other hours, on U.S. holidays, and on weekends.

### Using encryption

We strongly urge you to encrypt sensitive information sent by email. Our public PGP key is available from [http://www.cert.org/CERT\\_PGP.key](http://www.cert.org/CERT_PGP.key)

If you prefer to use DES, please call the CERT hotline for more information.

### Getting security information

CERT publications and other security information are available from our web site <http://www.cert.org/>

To subscribe to the CERT mailing list for advisories and bulletins, send email to [majordomo@cert.org](mailto:majordomo@cert.org). Please include in the body of your message

subscribe cert-advisory

\* "CERT" and "CERT Coordination Center" are registered in the U.S. Patent and Trademark Office.

---

### NO WARRANTY

Any material furnished by Carnegie Mellon University and the Software Engineering Institute is furnished on an "as is" basis. Carnegie Mellon University makes no warranties of any kind, either expressed or implied as to any matter including, but not limited to, warranty of fitness for a particular purpose or merchantability, exclusivity or results obtained from use of the material. Carnegie Mellon University does not make any warranty of any kind with respect to freedom from patent, trademark, or copyright infringement.

---

Conditions for use, disclaimers, and sponsorship information

Copyright 2002 Carnegie Mellon University.

### Revision History

July 22, 2002: Initial release

-----BEGIN PGP SIGNATURE-----

Version: PGP 6.5.8

Cert: CERT Advisory CA-2002-21 Vulnerability in PHP

iQCVAwUBPTyOVqCVPMXQI2HJAQGK6QQAp1rR7K18PNxpQZvqKPYWxyrtpiT8mmKN  
UuyERmOoX+5MAwH0hbAWCvVcyLH0gKGbTpBkRgToT8IEHZojwHCzqOaMM9kni/FG  
QEVeZnLfBX4GIgZGPu0XWlph3ZqaayWln57eGueYZ26zBuriIUu2cUCmyYGQkqII  
tuZdnDqUmR0=  
=+829  
-----END PGP SIGNATURE-----

---

- **Previous message:** CERT Advisory: "CERT Advisory CA-2002-21 Vulnerability in PHP"
- **Messages sorted by:** [ date ] [ thread ] [ subject ] [ author ] [ attachment ]