Security hole in PHP - Security

NEWS_PDF_AUTHOR: onokazu

NEWS_PDF_DATE: 2002/2/28 13:05:19

A security issue was found in all versions of PHP, including 3.x and 4.x versions. If you are running PHP on your server (i'm sure you all here are ), either upgrade your php or install the patch found at php.net. If you can't upgrade your php, because your site is hosted by an ISP, tell them to do so as soon as possible. This is NOT a security hole of XOOPS. It doesn't matter which php script you use on your server, since this is a problem in PHP itself. -- Update -- By BoobToob, Thursday Feb. 28th, 2002 Please read the full text of this artile. I posted the submission from Security Focus that gets very specific about what versions of PHP are affected and how to plug your current holes. I'm sending this to my ISP as we speak. Eric Caldwell aka BoobToob

To: BugTraq Subject: Advisory 012002: PHP remote vulnerabilities Date: Feb 27 2002 11:30AM Author: Message-ID: e-matters GmbH http://www.e-matters.de http://online.securityfocus.com/archive/1/258662 -= Security Advisory =- Advisory: Multiple Remote Vulnerabilites within PHP's fileupload code Release Date: 2002/02/27 Last Modified: 2002/02/27 Author: Stefan Esser [s.esser@e-matters.de] Application: PHP v3.10-v3.18, v4.0.1-v4.1.1 Severity: Several vulnerabilities in PHP's fileupload code allow remote compromise Risk: Critical Vendor Status: Patches Released Reference: http://security.e-matters.de/advisories/012002.html Overview: We found several flaws in the way PHP handles multipart/form-data POST requests. Each of the flaws could allow an attacker to execute arbitrary code on the victim's system. Details: PHP supports multipart/form-data POST requests (as described in RFC1867) known as POST fileuploads. Unfourtunately there are several flaws in the php_mime_split function that could be used by an attacker to execute arbitrary code. During our research we found out that not only PHP4 but also older versions from the PHP3 tree are vulnerable. The following is a list of bugs we found: PHP 3.10-3.18 - broken boundary check (hard to exploit) - arbitrary heap overflow (easy exploitable) PHP 4.0.1-4.0.3pl1 - broken boundary check (hard to exploit) - heap off by one (easy exploitable) PHP 4.0.2-4.0.5 - 2 broken boundary checks (one very easy and one hard to exploit) PHP 4.0.6-4.0.7RC2 - broken boundary check (very easy to exploit) PHP 4.0.7RC3-4.1.1 - broken boundary check (hard to exploit) Finally I want to mention that most of these vulnerabilities are exploitable only on linux or solaris. But the heap off by one is only exploitable on x86 architecture and the arbitrary heap overflow in PHP3 is exploitable on most OS and architectures. (This includes *BSD) Users running PHP 4.2.0-dev from cvs are not vulnerable to any of the described bugs because the fileupload code was completly rewritten for the 4.2.0 branch. Proof of Concept: e-matters is not going to release exploits for any of the discovered vulnerabilities to the public. Vendor Response: Because I am part of the php developer team there is not much I can write here... 27th February 2002 - An updated version of php and the patch for these vulnerabilities are now available at: http://www.php.net/downloads.php Recommendation: If you are running PHP 4.0.3 or above one way to workaround these bugs is to disable the fileupload support within your

php.ini (file_uploads = Off) If you are running php as module keep in mind to restart the webserver. Anyway you should better install the fixed or a properly patched version to be safe. Sidenotice: This advisory is so short because I don't want to give out more info than is needed. Users running the developer version of php (4.2.0-dev) are not vulnerable to these bugs because the fileupload support was completly rewritten for that branch. GPG-Key: http://security.e-matters.de/gpg_key.asc pub 1024D/75E7AAD6 2002-02-26 e-matters GmbH - Securityteam Key fingerprint = 43DD 843C FAB9 832A E5AB CAEB 81F2 8110 75E7 AAD6

A security issue was found in all versions of PHP, including 3.x and 4.x versions. If you are running PHP on your server (i'm sure you all here are ), either upgrade your php or install the patch found at php.net. If you can't upgrade your php, because your site is hosted by an ISP, tell them to do so as soon as possible. This is NOT a security hole of XOOPS. It doesn't matter which php script you use on your server, since this is a problem in PHP itself. -- Update -- By BoobToob, Thursday Feb. 28th, 2002 Please read the full text of this artile. I posted the submission from Security Focus that gets very specific about what versions of PHP are affected and how to plug your current holes. I'm sending this to my ISP as we speak. Eric Caldwell aka BoobToob

To: BugTraq Subject: Advisory 012002: PHP remote vulnerabilities Date: Feb 27 2002 11:30AM Author: Message-ID: e-matters GmbH http://www.e-matters.de http://online.securityfocus.com/archive/1/258662 -= Security Advisory =- Advisory: Multiple Remote Vulnerabilites within PHP's fileupload code Release Date: 2002/02/27 Last Modified: 2002/02/27 Author: Stefan Esser [s.esser@e-matters.de] Application: PHP v3.10-v3.18, v4.0.1-v4.1.1 Severity: Several vulnerabilities in PHP's fileupload code allow remote compromise Risk: Critical Vendor Status: Patches Released Reference: http://security.e-matters.de/advisories/012002.html Overview: We found several flaws in the way PHP handles multipart/form-data POST requests. Each of the flaws could allow an attacker to execute arbitrary code on the victim's system. Details: PHP supports multipart/form-data POST requests (as described in RFC1867) known as POST fileuploads. Unfourtunately there are several flaws in the php_mime_split function that could be used by an attacker to execute arbitrary code. During our research we found out that not only PHP4 but also older versions from the PHP3 tree are vulnerable. The following is a list of bugs we found: PHP 3.10-3.18 - broken boundary check (hard to exploit) - arbitrary heap overflow (easy exploitable) PHP 4.0.1-4.0.3pl1 - broken boundary check (hard to exploit) - heap off by one (easy exploitable) PHP 4.0.2-4.0.5 - 2 broken boundary checks (one very easy and one hard to exploit) PHP 4.0.6-4.0.7RC2 - broken boundary check (very easy to exploit) PHP 4.0.7RC3-4.1.1 - broken boundary check (hard to exploit) Finally I want to mention that most of these vulnerabilities are exploitable only on linux or solaris. But the heap off by one is only exploitable on x86 architecture and the arbitrary heap overflow in PHP3 is exploitable on most OS and architectures. (This includes *BSD) Users running PHP 4.2.0-dev from cvs are not vulnerable to any of the described bugs because the fileupload code was completly rewritten for the 4.2.0 branch. Proof of Concept: e-matters is not going to release exploits for any of the discovered vulnerabilities to the public. Vendor Response: Because I am part of the php developer team there is not much I can write here... 27th February 2002 - An updated version of php and the patch for these vulnerabilities are now available at: http://www.php.net/downloads.php Recommendation: If you are running PHP 4.0.3 or above one way to workaround these bugs is to disable the fileupload support within your php.ini (file_uploads = Off) If you are running php as module keep in mind to restart the webserver. Anyway you should better install the fixed or a properly patched version to be safe. Sidenotice: This advisory is so short because I don't want to give out more info than is needed. Users running the developer version of php (4.2.0-dev) are not vulnerable to these bugs because the fileupload support was completly rewritten for that branch. GPG-Key: http://security.e-matters.de/gpg_key.asc pub 1024D/75E7AAD6 2002-02-26 e-matters GmbH - Securityteam Key fingerprint = 43DD 843C FAB9 832A E5AB CAEB 81F2 8110 75E7 AAD6