

[VulnWatch] iDefense Security Advisory 03.15.07: Horde Project Cleanup Script Arbitrary File Deletion Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2007-03/msg00011.html>

- *From:* iDefense Labs <labs-no-reply@xxxxxxxxxxxxx>
 - *Date:* Thu, 15 Mar 2007 12:54:17 -0400
-

Horde Project Cleanup Script Arbitrary File Deletion Vulnerability

iDefense Security Advisory 03.15.07
<http://labs.iddefense.com/intelligence/vulnerabilities/>
Mar 15, 2007

I. BACKGROUND

The Horde Project provides a PHP-based framework, as well as applications for web-based group collaboration. IMP is their web-mail application. More information is available from the Horde Project web site at the following URL.

<http://www.horde.org/>

II. DESCRIPTION

Local exploitation of an input processing vulnerability within Horde Project's Horde and IMP allows attackers to delete arbitrary files.

This vulnerability specifically exists due to the improper handling of the output from an execution of `find(1)`. The output from `find(1)` is passed directly to a "for X in Y; do" as the Y value. Since the Y value is delimited by spaces, the for loop will process files containing spaces in their path as separate files. An attacker can create a file path containing spaces to manipulate the output from `find(1)`.

For example, creating the file `"/tmp/x /etc/passwd /tmp/mswordx"`, the following files will be deleted by the cron script; `"/tmp/x"`, `"/etc/passwd"`, and `"/tmp/mswordx"`.

III. ANALYSIS

Exploitation allows attackers to delete arbitrary files with the privileges of the user configured to run the cron script. Since a specially created path must be created on the local file system, local access is required.

In some cases this script may be installed to run as root. If installed with lesser privileges, such as that of the web server, this vulnerability is not quite as severe.

By deleting arbitrary files an attacker could possibly remove access controls, deny access to the system, or reset configurations. In some cases, it may be possible for an attacker to gain elevated privileges from this vulnerability.

IV. DETECTION

iDefense has confirmed the existence of this vulnerability in the cleanup cron scripts included in the following software packages:

Horde Framework; versions 3.0, 3.0.4, 3.1.3

Horde IMP; versions 2.0.8, 2.0.9, 2.2.8, 2.3.6, 3.0, 3.1, 3.2.1, 3.2.6, 3.2.8

The cleanup script was originally contained within the IMP package. The script was moved into the Horde Framework with the release of Horde Framework (H3) 3.0.

V. WORKAROUND

Disabling the vulnerable cron script will effectively prevent exploitation of this vulnerability.

VI. VENDOR RESPONSE

The Horde Project has corrected the vulnerable cron script within version 3.1.4 of the Horde Application Framework.

VII. CVE INFORMATION

A Mitre Corp. Common Vulnerabilities and Exposures (CVE) number has not been assigned yet.

VIII. DISCLOSURE TIMELINE

03/07/2007 Initial vendor notification

03/07/2007 Initial vendor response

03/15/2007 Coordinated public disclosure

IX. CREDIT

The discoverer of this vulnerability wishes to remain anonymous.

Get paid for vulnerability research

<http://labs.iddefense.com/methodology/vulnerability/vcp.php>

Free tools, research and upcoming events
<http://labs.idefense.com/>

X. LEGAL NOTICES

Copyright © 2007 iDefense, Inc.

Permission is granted for the redistribution of this alert electronically. It may not be edited in any way without the express written consent of iDefense. If you wish to reprint the whole or any part of this alert in any other medium other than electronically, please e-mail customerservice@xxxxxxxxxxxxx for permission.

Disclaimer: The information in the advisory is believed to be accurate at the time of publishing based on currently available information. Use of the information constitutes acceptance for use in an AS IS condition. There are no warranties with regard to this information. Neither the author nor the publisher accepts any liability for any direct, indirect, or consequential loss or damage arising from use of, or reliance on, this information.