

[UNIX] CDE Mailer argv[0] Format String

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-08/0085.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 08/26/04

To: list@securiteam.com

Date: 26 Aug 2004 10:55:24 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

CDE Mailer argv[0] Format String

SUMMARY

CDE Mailer (dtmail) is "a mail user agent (MUA) for CDE, which is installed on Solaris 8 and 9 by default. It provides an intuitive, easy-to-use GUI for reading, sending, and managing electronic mail".

CDE Mailer suffers from a format string vulnerability due to improper usage of a formatted print function.

DETAILS

Description:

Exploitation of a format string vulnerability in the dtmail binary included with CDE can allow local attackers to gain mail group privileges.

The vulnerability specifically exists due to improper usage of a formatted print function that allows a user supplied format to be processed via the argv[0] value. Local attackers can specify a special argv[0] containing format string characters to trigger the vulnerability and execute arbitrary code. Program arguments are copied onto the heap before being processed, so systems with non-executable stack protection are also easily affected.

Securiteam: [UNIX] CDE Mailer argv[0] Format String

Analysis:

Successful exploitation leads to group mail access. CDE is a widely deployed default desktop environment for UNIX operating systems. Gaining the ability to read other user email accounts, including root, could lead to exposure of highly sensitive data. The vulnerability is easily exploitable even when stack protections are enabled, furthering the impact of exposure.

Detection:

iDEFENSE has confirmed the existence of this vulnerability in Solaris 8 and Solaris 9. It is believed that this vulnerability only affects the Solaris implementation of CDE Mailer.

Vendor Status:

The Sun advisory for this issue (SunAlert #57627) is available at:
<<http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F57627>>
<http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F57627>

ADDITIONAL INFORMATION

The information has been provided by
<<mailto:idlabs-advisories@idefense.com>> iDEFENSE Labs.
The original article can be found at:
<www.idefense.com/application/poi/display?id=132&type=vulnerabilities>
www.idefense.com/application/poi/display?id=132&type=vulnerabilities

=====

This bulletin is sent to members of the SecuriTeam mailing list.
To unsubscribe from the list, send mail with an empty subject line and body to:
list-unsubscribe@securiteam.com
In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====
=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.
In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.