

[UNIX] SCO Unixware Setuid ptrace Local Privilege Escalation

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-02/msg00076.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxxx>
 - *Date:* 27 Feb 2006 19:06:16 +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>

SCO Unixware Setuid ptrace Local Privilege Escalation

SUMMARY

<<http://www.caldera.com/products/unixware>> SCO Unixware is a Unix operating system that runs on many OEM platforms.

Local exploitation of an access validation error in SCO Unixware allows attackers to gain root privileges.

DETAILS

Vulnerable Systems:

* SCO Unixware 7.1.3 and 7.1.4. (previous versions are suspected to be vulnerable.)

The vulnerability specifically exists due to a failure to check permissions on traced executables. The ptrace() system call provides an interface for debugging other processes on the system. SCO Unixware's implementation of the ptrace system call fails to check for setuid permissions on binaries before attaching to the process. This results in the complete control of memory and execution for the traced process with root privileges. Attackers can inject data into the running setuid process

[UNIX] SCO Unixware Setuid ptrace Local Privilege Escalation

and execute arbitrary code with root permissions.

Exploitation of this vulnerability is trivial. Simply placing shellcode in the environment and changing the instruction pointer via ptrace() is enough to elevate privileges.

Workaround:

It is not possible to reduce the impact of this vulnerability other than to restrict access to the affected systems.

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2934>>
CAN-2005-2934

Disclosure Timeline:

- * 15.09.05 – Initial vendor notification
- * 13.10.05 – Initial vendor response
- * 24.01.06 – Public disclosure

ADDITIONAL INFORMATION

The information has been provided by iDefense.

The original article can be found at:

<<http://www.iddefense.com/intelligence/vulnerabilities/display.php?id=395>>
<http://www.iddefense.com/intelligence/vulnerabilities/display.php?id=395>

=====

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@xxxxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxx

=====

=====

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.