

[UNIX] Usermin Remote Arbitrary Shell Command Execution Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-09/0021.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 09/09/04

To: list@securiteam.com

Date: 9 Sep 2004 12:12:20 +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>

Usermin Remote Arbitrary Shell Command Execution Vulnerability

SUMMARY

" <<http://www.webmin.com/index6.html>> Usermin is a web interface that can be used by any user on a Unix system to easily perform tasks like reading mail, setting up SSH or configuring mail forwarding. It can be thought of as a simplified version of Webmin designed for use by normal users rather than system administrators."

A vulnerability in Usermin's Web mail function could result in arbitrary OS command execution upon viewing a specially crafted HTML mail.

DETAILS

Vulnerable Systems:

- * Usermin version 1.070
- * Usermin version 1.080

Immune Systems:

- * Usermin version 1.090

A vulnerability exists in Usermin because the module responsible for mail

Securiteam: [UNIX] Usermin Remote Arbitrary Shell Command Execution Vulnerability

transmission fails to sanitize HTML mails including a link to another Usermin module. An attacker could take advantage of this problem to execute arbitrary OS commands with the privileges of the Usermin user.

Patch Availability:

Users are encouraged to upgrade their Usermin system to the newer version 1.090.

ADDITIONAL INFORMATION

The information has been provided by <mailto:snsadv@lac.co.jp> snsadv.

=====

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.