

[UNIX] Remote Buffer Overflow Vulnerability in IRIX SNMP Daemon

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-04/0008.html>

From: support@securiteam.com

Date: 04/04/02

From: support@securiteam.com

To: list@securiteam.com

Date: Thu, 4 Apr 2002 10:34:55 +0200 (CEST)

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

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> -- Know that you're safe.

Remote Buffer Overflow Vulnerability in IRIX SNMP Daemon

SUMMARY

Internet Security Systems (ISS) X-Force has discovered a buffer overflow in the SNMP (Simple Network Management Protocol) daemon in the SGI IRIX operating system. The SNMP daemon, or snmpd executable, runs with superuser privilege. The buffer overflow vulnerability in snmpd may allow remote attackers to execute arbitrary commands on a target system with elevated privileges.

DETAILS

Affected Versions:

SGI IRIX 6.5-6.5.15m and 6.5.15f

Note: Versions prior to version 6.5 may be vulnerable, but these versions are no longer supported by SGI.

SNMP is a widely used protocol used to remotely manage computers, networking devices, and applications. Many popular operating systems also contain SNMP functionality so computers can be managed over the network. SNMP is a lightweight, extensible protocol designed to facilitate remote management of devices. Most commonly, SNMP is used to monitor parameters

Securiteam: [UNIX] Remote Buffer Overflow Vulnerability in IRIX SNMP Daemon

of managed devices, such as determining a device's performance, if it is operational, or the general health of the device.

A vulnerability exists in the SGI IRIX implementation of snmpd that may allow remote attackers to submit a specially crafted SNMP request to cause a buffer overflow fault. This condition may be exploited to execute arbitrary code or commands on the target system.

The SNMP daemon is enabled by default on the IRIX operating system and is executed during the start-up sequence by the root user. The SNMP daemon accepts remote queries by default.

Recommendations:

ISS X-Force encourages affected users to apply vendor-supplied patches immediately. SGI has made patch 4574 available to remove the vulnerability described in this advisory. The SGI Software Product Knowledge Database is available at the following address: <http://support.sgi.com/spk/>

To limit access to SNMP at the firewall, filter port 1161 and 161 UDP/TCP. Consider disabling the SNMP daemon completely if it is not being used.

ADDITIONAL INFORMATION

The information has been provided by xforce@iss.net X-Force.

=====

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.

-
- **Previous message:** support@securiteam.com: "[NT] Quik-Serv Web Server Arbitrary File Disclosure"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)