

# [NEWS] HP ProCurve Switch Denial of Service Attack

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-07/0124.html>

---

*From:* [support@securiteam.com](mailto:support@securiteam.com)

*Date:* 07/28/02

From: [support@securiteam.com](mailto:support@securiteam.com)

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: Sun, 28 Jul 2002 08:21:49 +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.

-----

HP ProCurve Switch Denial of Service Attack

---

## SUMMARY

HP ProCurve Switches are the leading products in the switching market offered by Hewlett Packard. A security vulnerability in the product allows attackers to issue a special SNMP Write command that will cause the switch to crash upon contact with an HTTP or Telnet client.

## DETAILS

Vulnerable systems:

\* Hewlett Packard (HP) ProCurve Switch (HP J4121A ProCurve Switch 4000M revision C.07.23, ROM C.06.01)

HP Bug ID:

Not assigned

HP's SNMP variable (.iso.3.6.1.4.1.11.2.36.1.1.2.1.0) accessible by a simple SNMP WRITE with 85 characters crashes the ProCurve Switch upon its next connection with a Telnet or HTTP client.

Vendor status:

06/29/02 Initial Notification, [security-alert@hp.com](mailto:security-alert@hp.com) \*Note-Initial

Securiteam: [NEWS] HP ProCurve Switch Denial of Service Attack

notification by phenoelit includes a cc to [cert@cert.org](mailto:cert@cert.org) by default  
06/29/02 RBL blocked delivery to [security-alert@hp.com](mailto:security-alert@hp.com)  
06/29/02 Creation of ho-mail account and retransmission  
06/29/02 Auto-responder reply  
07/01/02 Human contact, PGP exchange and acknowledge.  
07/01/02 Clarification of some details w/HP Sec people  
07/19/02 Notification of intent to post publicly in approximately 7 days.  
07/23/02 Coordination for release date/times

Example:

```
linux# snmpwrite <switch_ip> private .iso.3.6.1.4.1.11.2.36.1.1.2.1.0 s  
`perl -e 'print "A"x85;`
```

ADDITIONAL INFORMATION

The information has been provided by <<mailto:fx@phenoelit.de>> X,  
<<mailto:kim0@phenoelit.de>> kim0, and <<mailto:zet@darklab.org>> Zet.

=====

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](mailto:list-unsubscribe@securiteam.com)

In order to subscribe to the mailing list, simply forward this email to: [list-subscribe@securiteam.com](mailto: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](mailto:support@securiteam.com): "[\[NEWS\] Ascend's Undocumented Protocol Allows Unauthorized Modifications](#)"
  - **Messages sorted by:** [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)