

[NEWS] IP3 NetAccess Arbitrary File Disclosure

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-02/msg00031.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 12 Feb 2007 16:39:09 +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>

IP3 NetAccess Arbitrary File Disclosure

SUMMARY

<<http://www.ip3.com/pooverview.htm>> IP3's NetAccess is a device created for high demand environments such as convention centers or hotels. It handles the Internet access and provides for instance firewalling, billing, rate-limiting as well as various authentication mechanisms. The device is administrated via SSH or a web-based GUI.

An arbitrary file disclosure vulnerability in IP3 NetAccess leads to full system compromise.

DETAILS

Vulnerable Systems:

* NetAccess devices with a firmware version less than 4.1.9.6

Due to improper input validation, all NetAccess devices with a firmware version less than 4.1.9.6 are vulnerable to an arbitrary file disclosure vulnerability. This vulnerability allows an unauthenticated remote attacker to abuse the web interface and read any file on the remote system. Due to the fact that important system files are world-readable (see bid #17698), this does include /etc/shadow and thus leads to a full

[NEWS] IP3 NetAccess Arbitrary File Disclosure

compromise of the device! In addition an attacker is able to gain access to the proprietary code base of the device and potentially identify as well as exploit other (yet unknown) vulnerabilities.

The trivial vulnerability can be exploited by accessing the file "getfile.cgi" with a relative file path such as [http://\\$target/portalgroups/portalgroups/getfile.cgi?filename=../../../../../../../../etc/shadow](http://$target/portalgroups/portalgroups/getfile.cgi?filename=../../../../../../../../etc/shadow)

As the input to the "filename" parameter is not properly validated accessing this URL will disclose the contents of /etc/shadow to a remote attacker.

Fix:

To address this problem, the vendor has released a new firmware version (4.1.9.6) which is available at <http://www.ip3.com>. Hence all users of IP3's NetAccess devices are asked to install this version immediately.

Workaround:

As a temporary workaround, one may also limit the accessibility of the web interface of the device to authorized personnel only. Nevertheless contacting the vendor and installing the new firmware version is highly recommended!

Disclosure Timeline:

- * 31 December 2006 – Notified vendor
- * 31 December 2006 – Vulnerability confirmed
- * 17 January 2007 – Patch released
- * 11 February 2007 – Public disclosure

ADDITIONAL INFORMATION

The information has been provided by <<mailto:sebastian@xxxxxxxxxxxxxxxx>> Sebastian Wolfgarten.

The original article can be found at:

<<http://www.devtarget.org/ip3-advisory-02-2007.txt>>

<http://www.devtarget.org/ip3-advisory-02-2007.txt>

<<http://www.milw0rm.com/exploits/3294>>

<http://www.milw0rm.com/exploits/3294>

=====

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

[NEWS] IP3 NetAccess Arbitrary File Disclosure

=====
=====

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.