Security Research Advisory

Siemens SANTIS 50

Authentication Issue

Table of Contents

Authentication Issue					Advisory Number
					SN-05-01
Severity	Software	Version(s)	Accessibility	CVE	Author(s)
M	Siemens Santis 50 Wireless Router	Firmware v4.2.8.0	Remote	-	Luca Carettoni
	Vendor URL		Advisory URL		
	-		-		

Date	Details
17/07/2005	Vendor disclosure
-	Vendor acknowledgment
-	Patch release
25/07/2005	Public disclosure

Summary

The Siemens Santis 50 Wireless router is a wi-fi (802.11b) ADSL router. It's a complete system for home and small business networks in a single device.

Some features include: - Integrated WLAN for internet sharing - ADSL Modem/Router/Firewall/Switch - 10/100 Mbps 4 port switch built in - Stateful packet inspection (SPI) firewall - Wireless Access Point - VPN passthrough Telecom Italia Net (one of the largest italian Internet providers) delivers this device to its ADSL customers, so in Italy it's a common device used in SOHO and SMB networks.

The Siemens Santis50, the Ericsson HN294dp and the Dynalink RTA300W devices share the same hardware, so it's very likely that they share this vulnerability. The original project of these products was from Askey. The firmware software is from ViirataGlobespan, bought by Conexant.

The tested (vulnerable) version of firmware is the 4.2.8.0

This bug provides access to the management CLI, without authentication, after a DOS attack to a specific service port.

Vulnerability Details

This device provides a web management interface and the classic telnet CLI for administration purposes. By default these services are available only from the local network, but can be optionally activated also on the WAN interface.

Sending trigger packets to the management port (280/http-mgmt), the device "freezes" the web interface, allowing unauthenticated connection to the telnet CLI.

This behavior appears to be some sort of "disaster recovery mode". The set of available commands is limited to a few, but they are enough to discover information about the configuration of the device and connections (events, traffic, ethernet addresses configuration, etc). Also, critical commands like "irreversibly erase FLASH contents" are available.

A vendor-provided fix is currently unavailable. An upgrade to a more recent version of firmware (v5.2.2 is currently available) could help, but we are unable to test this version.

An obvious workaround (and good practice) is to disable the management interface on the WAN, this obviously blocks this attack from external attackers.

Technical Details

Description

A simple exploit is to use the application scanner AMAP (kudos to THC, www.thc.org).

```
$ amap x.x.x.x 280
```

Legal Notices

Secure Network (www.securenetwork.it) is an information security company, which provides consulting and training services, and engages in security research and development.

We are committed to open, full disclosure of vulnerabilities, cooperating with software developers for properly handling disclosure issues.

The information in the advisory is believed to be accurate at the time of publishing based on currently available information. This information is provided as-is, as a free service to the community by Secure Network research staff. There are no warranties with regard to this information. Secure Network does not accept any liability for any direct, indirect, or consequential loss or damage arising from use of, or reliance on, this information.

If you have any comments or inquiries, or any issue with what is reported in this advisory, please inform us as soon as possible.

e-mail	info@securenetwork.it
phone	+39 02 917 730 41