

# [NEWS] Multiple Red-M 1050 Blue Tooth Access Point Vulnerabilities

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-06/0021.html>

---

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

*Date:* 06/06/02

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

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

Date: Thu, 6 Jun 2002 07:30:07 +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.

-----

Multiple Red-M 1050 Blue Tooth Access Point Vulnerabilities

---

## SUMMARY

<<http://www.red-m.com>> Red-M's 1050AP (Bluetooth Access Point) is the device which exists between legacy Ethernet networks and Bluetooth 1.0/1.1 compatible devices looking to obtain IP network access. Red-M's device is currently the only device that supports piconet (multiple Bluetooth clients to one access point).

A number of vulnerabilities exist, which are outlined below, that could enable an attacker on the wired or wireless side of the device to mount an attack against the device in an attempt to locate the device, cause loss of administration functionality or compromise the administration interface.

## DETAILS

Vulnerable systems:

- \* Red-M 1050AP (Bluetooth Access Point)
- \* 1050AP boot v01.03.16
- \* 1050AP loader v02.01.26
- \* 1050AP software v02.00.26

## Securiteam: [NEWS] Multiple Red-M 1050 Blue Tooth Access Point Vulnerabilities

### Issues:

- \* Red-M 1050 Access Point Management Web Server DoS
- \* Red-M 1050 Access Point Case Insensitive Passwords
- \* Red-M 1050 Access Point TFTP Server Based Password Attack
- \* Red-M 1050 Access Point Management Session State Storage
- \* Red-M 1050 Access Point Device Existence Broadcast
- \* Red-M 1050 Access Point PPP Denial of Service

### Severity:

An attacker is able to disable the administration web server, crack the administration password via TFTPd (UDP), piggyback-authorized administration connections when proxied, NAT addresses are in use, and locate device on network without requiring scanning the network to locate it.

#### [1] Red-M 1050 Access Point Management Web Server DoS

The 1050AP device provides a web based management interface to allow configuration of the device. This web based management system has no concept of authorized or unauthorized hosts and is simply protected by a password over an unencrypted connection.

There exists a vulnerability in the web server that runs on the 1050AP that potentially allows an attacker to disable the web server completely until the device is restarted (physically).

#### [2] Red-M 1050 Access Point Case Insensitive passwords

Another existing vulnerability in the AP is that the administration password is not case sensitive. This combined with the fact that the maximum password length is 16 chars (documented) and can only be a-z, 0-9 (@stake testing) greatly reduces the number of passwords which can be used and thus reduces cracking time.

#### [3] Red-M 1050 Access Point TFTP Sever Based Password Attack

In addition, the AP provides a TFTPd server for configuration backups and firmware updates. This TFTPd server cannot be disabled and can be used by an attacker to crack the administration password using a UDP based attack. This combined with the above can provide an effective way of cracking the administration password in a short time by either dictionary or brute force methods.

#### [4] Red-M 1050 Access Point Management Session State Storage

There exists another vulnerability within the administration web interface. When you login with the admin password to the web interface, no cookie, session ID or basic authentication data are passed. No data is passed from the client either to server or from the server to the client in response to maintain state of the current session. The server simply remembers that your IP successfully logged in until the session expires and/or you click the logout button. This method of maintaining state suffers from a number of attacks:

I) You connect to the device via a proxy; then any user who uses the same proxy can connect to the admin interface already authenticated.

## Securiteam: [NEWS] Multiple Red-M 1050 Blue Tooth Access Point Vulnerabilities

II) You connect to the device via a firewall which does NAT/PAT; then, as above, anyone who is NAT'd behind the same IP can get access to the admin interface.

III) A number of other IP/Layer2 based attacks for traffic redirection or forged packets are possible.

This combined with the fact that when changing the administration password, the device does not ask for the current password. This means that an Administrator can effectively be locked out of the device by an attacker successfully exploiting this vulnerability.

### [5] Red-M 1050 Access Point Device Existence Broadcast

The device broadcasts its name via UDP to the broadcast address (255.255.255.255). Therefore, to detect a Red-M AP active on the network simply listen on UDP port 8887, and every minute or so a broadcast will occur which delivers the following information: the AP's current name, IP address, netmask, serial number, and aerial address.

### [6] Red-M 1050 Access Point PPP Denial of Service

Finally, it is possible for an attacker who is bonded to cause a denial of service within the AP. Each attempt to connect thereafter will not work, simply generating an error of 'Unable to establish a connection' within the Microsoft dial-up connection dialog box.

#### Details:

It should be noted that although a number of issues are listed as DoS-only, this is only limited by the fact that during the assessment of the device @stake was unable to gain access to the debugging interface to enable the successful exploitation of the vulnerabilities (be they buffer or heap overflows).

### [1] Red-M 1050 Access Point Management Web Server DoS

Connect to the web interface and enter a long string for the administration password. Click 'OK'. You will get a connect error on the page refresh and the web server will be dead until you power down the device and restart it physically.

### [2] Red-M 1050 Access Point Case Insensitive passwords

The same file was requested twice using the different cases. In each case, the same file was returned. This can also be demonstrated within the web interface by attempting to login with either the real password or the same password but using a different case (e.g. AbCdEf instead of abcdef).

```
C:\>tftp -i 192.168.1.253 get FLASH_Database-abcdef  
Transfer successful: 381 bytes in 2 seconds, 190 bytes/s
```

```
C:\>tftp -i 192.168.1.253 get FLASH_Database-AbCdEf FLASH_Second  
Transfer successful: 381 bytes in 3 seconds, 127 bytes/s
```

```
C:\>fc FLASH_Database-abcdef FLASH_Second  
Comparing files FLASH_Database-abcdef and FLASG_Second
```

## Securiteam: [NEWS] Multiple Red-M 1050 Blue Tooth Access Point Vulnerabilities

FC: no differences encountered

### [3] Red-M 1050 Access Point TFTP Sever Based Password Attack

Simply execute the following command replacing the <password> tag with the attempted password.

```
tftp -i 192.168.1.1 get FLASH_Database-<password>
```

### [4] Red-M 1050 Access Point Management Session State Storage

A simple way to demonstrate this vulnerability is to use one browser (such as IE) and authenticate with the management interface. Then load a different browser (such as Netscape) and then type in the address of the AP. You will be presented with the pre-authenticated administrative interface on the AP.

### [5] Red-M 1050 Access Point Device Existence Broadcast

Use a tool such as netcat to listen on port UDP/8887 (i.e. nc -u -L -p 8887 -o output). Every 30 seconds a new entry will be made in the log file similar to the one below:

```
< 00000000 2c 01 be ba c0 a8 01 fd ff ff ff 00 00 02 81 64 #  
&....2.....d  
< 00000010 00 56 02 06 08 01 00 00 00 0d 01 57 6f 6c 6c 79 #  
V.....Wolly  
< 00000020 57 6f 72 6c 64 00 # World.
```

A break down of the packet is as follows:

- [bytes 1] Length of data segment of packet
- [bytes 2 to 4] Unknown
- [bytes 5 to 8] IP address of device
- [bytes 9 to 12] Subnet mask of device
- [bytes 13 to 15] Serial Number\*
- [bytes 16 to 18] Bluetooth Address\*
- [byte 19] Is the device configured (01 = no / 02 = yes)
- [bytes 20 to 27] Unknown
- [bytes 28 to LEN-1] Access point name

The above packet is how Red-M's own set up program knows of the AP's existence on the network.

\* [bytes 13 to 18] the aerial address

### [6] Red-M 1050 Access Point PPP Denial of Service

Bond and then connect with the AP. When prompted for the PPP username for the link enter a very long username.

Recommendation:

Upgrade your firmware to the latest release. In addition, follow the steps outlined below to mitigate the current design vulnerabilities.

Typically, wireless access points to the network should be considered hostile networks. In the case of the above vulnerabilities, a packet-filtering device should be placed between the Ethernet interface of

## Securiteam: [NEWS] Multiple Red-M 1050 Blue Tooth Access Point Vulnerabilities

the AP and the corporate network restricting the types of traffic and from which hosts communication destined for the AP can come from. However, this will still expose the device to attacks from the wireless side of the device. To guard against these attacks, ensure that good username and password policies are in place. However, consider the limitations of the username and passwords in the 1050AP. Strong passwords may not be possible. From @stake's testing, usernames and passwords can only be [a-z] and [0-9] within the device's PPP authentication mechanism.

The 1050AP does provide a number of other mechanisms to protect against being discovered and to protect against automatic connections. For details of these please refer to the vendor's documentation. It is @stake's recommendation that the following options are used:

[Option] [Suggested Setting]

Authentication: Authentication with bonding

Force encryption: Check box

Accessibility mode: Connectable and non discoverable

PPP authentication: Check box

Automatically authorize: Uncheck box

Vendor Response:

Red-M was initially notified of these vulnerabilities between August and November 2001.

It should be noted the DoS attacks have been resolved in the latest release of the firmware available from the Red-M website:

[http://www.red-m.com/Products/Downloads/freefiles/1050AP\\_2\\_02\\_10.zip](http://www.red-m.com/Products/Downloads/freefiles/1050AP_2_02_10.zip)  
[http://www.red-m.com/Products/Downloads/freefiles/1050AP\\_2\\_02\\_10.zip](http://www.red-m.com/Products/Downloads/freefiles/1050AP_2_02_10.zip)

The remaining design issues are due to be resolved in a firmware release planned for August 2002.

The following response was received from Red-M via email.

"We continue to see the principle new threat introduced by the addition of a wireless access point as being from outside that network, over the wireless(Bluetooth) interface, or an external connection to the wired network (typically the Internet). This is continuously re-enforced by the customer feedback we receive. We believe that your draft advisory does not demonstrate a practical vulnerability over the \*wireless\* interface, as the 1050AP's wireless security mechanisms (Bluetooth security) has not been shown to be vulnerable. The vulnerabilities that you have identified require that 1050AP is installed in an environment where the corporate security policy allows such attacks to be mounted on the wired side of the Access Point.

The current design philosophy for the 1050AP is that it would be used on a corporate network already secured by implementation of a corporate security policy. This should mitigate the risk of attacks from the wired network. We have thus concentrated on meeting the customer requirement of

Securiteam: [NEWS] Multiple Red-M 1050 Blue Tooth Access Point Vulnerabilities

securing access to the wired network from the wireless side by, for example, rogue Bluetooth devices.

However, we also realize that a level of security is required to mitigate some types of attack from inside the wired network, and to prevent accidental compromising of wireless connectivity. The issues you have raised we believe fit into this category. Revised firmware to address the issues you raised is now planned for the firmware release in August. This firmware will be applied both to new build of product and made available for the installed base as an upgrade that can be applied to product that's already in use."

ADDITIONAL INFORMATION

The information has been provided by <mailto:[ollie@atstake.com](mailto:ollie@atstake.com)> Ollie Whitehouse.

=====

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): "[NT] Multiple Vulnerabilities in Yahoo! Messenger"
- *Messages sorted by:* [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)