

Full-Disclosure: [Full-Disclosure] Bluetooth: BlueSnarf and BlueBug Full Disclosure

[Full-Disclosure] Bluetooth: BlueSnarf and BlueBug Full Disclosure

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2005-01/0001.html>

From: Adam Laurie (adam.laurie_at_thebunker.net)

Date: 12/31/04

Date: Fri, 31 Dec 2004 09:53:09 +0000

To: full disclosure <full-disclosure@lists.netsys.com>, bugtraq <bugtraq@securityfocus.com>, risk

BlueSnarf, BlueBug & HeloMoto Full Disclosure, December 2004

In November 2003, various vulnerabilities on Bluetooth enabled mobile phones emerged, as published here:

<http://www.thebunker.net/security/bluetooth.htm>

Details of the attacks were disclosed at the Chaos Computer Club's annual congress in Berlin – 21C3:

<http://www.ccc.de/congress/2004/fahrplan/event/66.en.html>

Slides from the talk can be found here:

http://trifinite.org/Downloads/21c3_Bluetooth_Hacking.pdf

Video of the talk will be on the CCC site in due course.

It was felt, as the industry had been given a full 13 months to react to the original threat discovery, and responsible manufacturers had engineered and released firmware upgrades, that the time had come for full disclosure. This became increasingly urgent as it was clear that the techniques used were becoming relatively widely known within the security community, and it could therefore be assumed that the same was true for criminal and/or malicious users.

Vendor Responses

Nokia's response page is here:

<http://www.nokia.com/nokia/0..56221.0.html>

It emerged at the conference that Nokia have created a special warranty

Full-Disclosure: [Full-Disclosure] Bluetooth: BlueSnarf and BlueBug Full Disclosure

code for the Bluetooth security issues, and any affected phone, regardless of age or origin, can be upgraded under that code free of charge. This was stated by a member of the audience during the presentation, and has not yet been verified.

Known affected devices: 6310, 6310i, 8910, 8910i

Sony Ericsson have not responded directly to the author, but have stated publicly that the problem has been fixed in all affected phones. This has not been verified, and availability of firmware upgrades is unknown.

Known affected devices: T68, T68i, R520m, T610, Z1010, Z600

Motorola stated that they are committed to fixing the problem, but further details are unknown.

Known affected devices: V80, V5xx, V6xx and E398.

I hope this is useful, and I wish you all a safe, happy and secure New Year!

cheers,
Adam

--

Adam Laurie
The Bunker Secure Hosting Ltd.
Shepherds Building
Rockley Road
London W14 0DA
UNITED KINGDOM

Tel: +44 (20) 7605 7000
Fax: +44 (20) 7605 7099
<http://www.thebunker.net>
mailto:adam@thebunker.net
PGP key on keyservers

Full-Disclosure - We believe in it.

Charter: <http://lists.netsys.com/full-disclosure-charter.html>