trifinite Security Advisory: Buffer Overrun in Toshiba Bluetooth Stack for Windows (TRSA00001)

Author: Martin Herfurt <martin.herfurt (at) trifinite.org>

Organization: trifinite.org

Web: http://trifinite.org/

trifinite Security Advisory: Buffer Overrun in Toshiba Bluetooth Stack for Windows (TRSA00001)

Summary

This advisory describes a vulnerability that affects Toshiba Bluetooth Host Stack implementations up to version 4.0.23.

A vulnerability has been discovered that enables the attacker to remotely perform a denial of service (DoS) against the host. This vulnerability was discovered by members of the trifinite.group (Martin Herfurt, Marcel Holtmann and Adam Laurie)

Affected Products

Hosts with the Toshiba Bluetooth Stack for Windows up to Version 4.0.23
Vulnerable Versions of this software ship with the following computers:

- Toshiba Computers with Bluetooth interface
- Dell Computers with Bluetooth module D350
- Sony Vaio Computers with Bluetooth Interface
- ASUS Computers with Bluetooth Interface
- and possibly other brands that use this stack

Details

The attacker is able to remotely cause a critical System Exception on Windows XP hosts that results in an immidiate reboot of the system (Blue Screen of Death). The crash is triggered through the host's Bluetooth interface by an attack that has been introduced under the name BlueSmack (http://trifinite.org/trifinite_stuff_bluesmack.html). By sending large payloads with L2CAP Echo Requests, data is written to non-paged memory areas. The driver causing this behaviour is TOSRFBD.SYS.

Impact

The attacker is able to remotely cause a critical system exception on Windows hosts that results in an immidiate reboot of the system (Bluescreen of Death). The attacker needs to be in physical proximity of the device. Depending on the Bluetooth device class, Bluetooth Wireless Technology typically covers a range 10 meters. This range can be extended to distances of up to one mile by using directional antennas that are connected to the attacker's equipment.

Obtaining Fixed Software

At the time of the publication of this advisory (20th of June 2006), the vendor had more than four months for resolving the issue and did not succeed. They have declined to comment on our submission. In the process of disclosure, Microsoft and the Bluetooth SIG have also been informed about the issue in April 2006.
At the time of writing this advisory, there is no version of the enhanced data rate (EDR) capable Toshiba Bluetooth Stack for Windows that is secure against the vulnerability described above. The latest version of the stack which has been released in May 2006 and does not address this vulnerability either.

Workarounds

As the attacker needs to know the Bluetooth device address of the host a workaround is to switch the Bluetooth module into invisible mode. This mode prevents the host from being discovered by attackers and allows normal operation of Bluetooth devices that are bonded with the host.

Exploitation and Public Announcements

Besides the ability to remotely cause a blue screen, the ability to execute arbitrary code on the accected machine cannot be confirmed.

Distribution

This advisory has been posted to the BugTraq, Full Disclosure and BlueTraq mailing lists and is available as pdf document in the downloads section of trifinite.org (http://trifinite.org/)

Revisison History

20th of June 2006: Initial release of document