

[VulnWatch] Windows URG mystery solved!

Source: <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2003-09/0022.html>

From: Michal Zalewski (lcamtuf_at_dione.ids.pl)

Date: 09/17/03

Date: Wed, 17 Sep 2003 11:17:16 +0200 (CEST)
To: bugtraq@securityfocus.com, vulnwatch@vulnwatch.org

I finally have more details about the Windows URG pointer memory leak, first reported here:

<http://www.securityfocus.com/archive/82/335845/2003-08-31/2003-09-06/0>

It is a vulnerability.

After a long and daunting hunt, I have determined that pretty much all up-to-date Windows 2000 and XP systems are vulnerable to the problem, and that it is not caused by any network devices en route or such, but the issue is present only in certain conditions.

I have initially reported I see a minority population of systems exhibiting this pattern. It turns out the majority of population is vulnerable, simply not exhibiting this behavior all the time.

It is exhibited whenever a data transfer is occurring at the time the initial SYN is sent. The URG value would often contain a random piece of a packet (frequently data) belonging to the other connection.

This happens during regular browsing, and will also be triggered by background downloads, etc.

I do not want to exaggerate the impact of this vulnerability, the amount of data disclosed is fairly low, but it's still quite cool.

Cheers,

```
--  
----- bash$ :(){ :|:&}:: --  
Michal Zalewski * [http://lcamtuf.coredump.cx]  
Did you know that clones never use mirrors?  
----- 2003-09-17 10:44 --
```