

Re: TCP RST attacks and Windows Servers

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.windows.server.security/2004-04/0245.html>

From: Karl Levinson [x y] mvp (levinson_k_at_despammed.com)

Date: 04/28/04

Date: Wed, 28 Apr 2004 00:48:50 -0400

Pretty much any and all system running Windows or another OS with IP v4 is vulnerable to spoofed TCP RST and SYN attacks to reset connections.

However, most client TCP implementations, including Windows TCP networking implementations including NetBIOS, would probably just retry the session and reconnect like nothing ever happened. This is why most people are discussing this vulnerability as a problem for BGP, where a number of dropped sessions might cascade to cause a significant problem.

Unless I am mistaken, there are various things you can do, such as SMB signing, IPsec security associations, and using ACLs on routers to prevent IP address spoofing from people that are not on that local subnet. I seem to think there are authentication things you can do with NetBIOS, both using IPsec and not using IPsec.

Note that it is not truly trivial to do these attacks. You must already know or guess the source and destination IP addresses and port numbers in use. If you are able to sniff this data, you might as well use that information to hijack the TCP session, instead of DoS it. People have been doing that for ages, with commonly known free tools.

Other much more common attacks such as ARP spoofing and other spoofing that can lead to man in the middle TCP session hijacking, remains a much more real concern than TCP DoSes for every OS out there. MITM hijacking tools for script kiddies have been around for years. If I was going to go to all the trouble to determine the source and destination IP addresses and port numbers, I would probably rather use that information to hijack the session and thus control the server, instead of do a weak DoS.

Last, an attack script to exploit this vulnerability has been out there for many days. If the Internet was going to go down via this script, you would think it should have happened by now.

"baillard" <baillard@hotmail.com> wrote in message
news:er5skH#JEHA.3924@tk2msftngp13.phx.gbl...
> *I have not seen anything yet from Microsoft about the TCP RST possible*
> *attacks that are detailed in the following bulletins:*
>

- > *Technical Cyber Security Alert TA04-111A*
- > *Vulnerabilities in TCP*
- > <http://www.us-cert.gov/cas/techalerts/TA04-111A.html>
- >
- > SANS
- >
- > <http://isc.incidents.org/diary.php?date=2004-04-20&isc=9a4c61bc294b1039c8ecacff03534c2c>
- > *CVE entry: <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0230>*
- > *Cisco announcement:*
- > <http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml>
- >
- > *If I understand correctly, an attack would affect any long term session*
- TCP
- > *communications. Since Windows Server 2003 and 2000 running as Domain*
- > *Controllers are not supported using IPSEC (one mentioned work around),*
- what
- > *possible attacks will we be facing in the future? Does standard Windows*
- > *networking (SMB) depend on this kind of communication? Can a Windows box*
- > *setup to do routing (I don't remember if RRAS supports BGP) be affected by*
- > *these kinds of attacks?*
- >
- >