

Re: TCP RST attack

Source: <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2004-04/0095.html>

From: Dag-Erling Smørgrav (*des_at_des.no*)

Date: 04/20/04

To: Mike Tancsa <mike@sentex.net>

Date: Tue, 20 Apr 2004 19:44:37 +0200

Mike Tancsa <mike@sentex.net> writes:

> <http://www.uniras.gov.uk/vuls/2004/236929/index.htm>

The advisory grossly exaggerates the impact and severity of this fea^H^H^Hbug. The attack is only practical if you already know the details of the TCP connection you are trying to attack, or are in a position to sniff it. The fact that you can attack a TCP connection which passes through a network you have access to sniff should not be a surprise to anyone; the remaining cases require spoofing of a type which egress filtering would prevent, if only people would bother implementing it.

I don't believe BGP sessions are as exposed as the advisory claims they are, either. The possibility of insertion attacks (which are quite hard) was predicted six years ago, when RFC 2385 (Protection of BGP Sessions via the TCP MD5 Signature Option) was written. RST attacks may cause route flapping, but that can be avoided with a short hysteresis (though this may be impractical for backbone routers)

Insertion attacks against SSL connections are practically impossible, so the only risk there is an RST attack, which most browsers should handle gracefully.

DNS connections (even zone transfers) are so short-lived that you would have to be very, very lucky to pull off an insertion or RST attack against.

The most likely attack scenario to come out of this is probably gamers and IRC weenies kicking eachother off servers (the server's IP address and port number are known, the servers often reveal client IP addresses to other clients, and the client often uses a fixed source port, or one from a relatively small range)

DES

--

Dag-Erling Smørgrav - des@des.no

FreeBSD-Security: Re: TCP RST attack

freebsd-security@freebsd.org mailing list

<http://lists.freebsd.org/mailman/listinfo/freebsd-security>

To unsubscribe, send any mail to "freebsd-security-unsubscribe@freebsd.org"