

RE: [Full-Disclosure] Sidewinder G2

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2003-11/0940.html>

From: Mike Fratto (mfratto_at_nwc.com)

Date: 11/20/03

To: "'Ron DuFresne'" <dufresne@winternet.com>, "'Brent J. Nordquist'" <b-nordquist@bethel.edu>
Date: Thu, 20 Nov 2003 12:37:41 -0500

>So, then I have to ask here; do you or anyone
> else know of a security incident that compromised the
> perimeter guarded by one of these blackboxen?

Yes, I did. Through the transparent HTTP application proxy in version 4.1, as I stated in an earlier email but...

>And I'd direct
> folks to the sec-focus vuln listings to determine how these
> systems have faired historically say since oh, 1995 or so.

If you not current with security software to the last two years your screwed anyway. A search at Cert for "Secure Computing" and "Sidewinder: yielded 6 entries, the earliest in 2002. A search at BugTraq db at security focus showed 0. Hrmmmm. The consistent response at Cert was that the vuln didn't yield anything useful due to Type Enforcement.

The SideWinder is a proxy firewall and it has application support many of the common protocols like HTTP, SMTP, FTP, telnet, SQL*Net, H.323, T.120, etc. What you need to remember is that even if the external proxy contains a vulnerability doesn't mean that traffic will be passed internal hosts. You also have to remember the limitations if application proxies, many only deal with protocol headers and don't even look into the protocol payload. So exploits against vulnerable servers are typically stopped because 1) the exploit contains characters outside of the set defined by RFC822 (aka binary characters ASCII 128-255) or can be contained by header length enforcement (do you really need a HTTP host: header length greater than 50 characters?). The application proxy can also limit commands to a subset, which is useful, but makes support for using TLS within SMTP impossible. Now there are still ways round this type of processing like sending ASCII encoded shellcode, but you might also bump into those pesky line length issues.

I have tested Sidewinder 4.1, 5.0, and G2 and for the most part it provided the protective functions that SecureComputing claimed. I tested G2 by trying to send illegal characters in the headers, overly long header lengths, and other manipulations none of which passed through to the internal network.

Full-Disclosure: RE: [Full-Disclosure] Sidewinder G2

So the real question is not "how secure sidewinder is" (or any product for that matter). The real question is what protective measures does the sidewinder provide AND how well are they implemented.

mike

Full-Disclosure – We believe in it.

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