

---

## SSL

Posted by gkkitag - 2003/11/04 20:15

---

How does GoGlobal use ssl? Specifically, I refer to <http://www.cert.org/advisories/CA-2003-26.html>.

Any information would be greatly appreciated.

=====

## Re: SSL

Posted by troym - 2003/11/04 21:15

---

How does GoGlobal use ssl? Specifically, I refer to <http://www.cert.org/advisories/CA-2003-26.html>.

GO-Global for UNIX uses a version of OpenSSL that is affected by the advisory you have linked to. You can disable the SSL port, and thus not be vulnerable by passing an "-sslport 0" argument to the "gold" daemon, or by specifying "GOLD\_SSL\_PORT=0" in the `#{GOGLOBAL_ROOT}/etc/gold.conf` file.

This set of vulnerabilities is scheduled to be addressed in the next point release of GO-Global for UNIX (v2.1.1). The estimated timeframe is a bit fluid as we are adding and removing requirements that will be included, but it should be in the first quarter of 2004, if not sooner. (This is not a guarantee and should only be considered a possibility, however.)

While GO-Global for UNIX is technically vulnerable to exploits as listed in the advisory, most users of our product use it on an isolated LAN environment (or over a VPN where access is controlled). As such, the server is not subject to attack from unknown intruders (such as a web server would be). In addition, the vulnerabilities are related to client certificate verification, which the GO-Global product does not currently do, so exposure is limited by this as well. Obviously none of this is intended as an excuse, let alone a good one, for not having addressed this vulnerability, but only a rationale as to why this has not been addressed to date.

Hope this helps,  
Troy

=====