clavister information

POODLE Attacks on SSLv3

Clavister informs – here's what you need to know

According to www.imperialviolet.org/2014/10/14/poodle.html there is a flaw inherent in the SSLv3 design. Clavister cOS Core has supported SSLv3 in previous releases, and more specifically in the Clavister HTTPS Web Management user interface, the TLS ALG and in the SSL VPN Client.

Since the problem is inherent in the actual SSLv3 protocol, there is no secure fix for the problem. Clavister has therefore opted to remove the SSLv3 option from all Clavister products and systems through a single correction release of all supported releases.

The supported releases are:

Clavister cOS Core 10.21.02
Clavister cOS Core 10.20.04
Clavister cOS Core 10.11.07

More details about the vulnerability:
web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-3566
www.imperialviolet.org/2014/10/14/poodle.html

clavister®
WE ARE NETWORK SECURITY

Clavister AB, Sjögatan 6 J, SE-891 60 Örnsköldsvik, Sweden
■ **Phone:** +46 (0)660 29 92 00 ■ **Fax:** +46 (0)660 122 50 ■ **Web:** www.clavister.com