clavister information

GHOST

Clavister Systems Not Affected

You may have heard this week about the 'GHOST' vulnerability (CVE-2015-0235), in the Linux GNU C Library (glibc). This vulnerability enables hackers to remotely take control of systems without even knowing any system IDs or passwords. Once an attacker has exploited GHOST they may be capable of taking over the entire system.

GHOST poses a remote code execution risk that makes it easy for an attacker to exploit a machine. This could be done via sending an email to a Linux-based system and automatically getting complete access to that machine.

This vulnerability exists in any Linux system that was built with `glibc-2.2`, which was released on November 10, 2000. Researchers found that the bug had actually been patched with a minor bug fix released on May 21, 2013 between the releases of `glibc-2.17` and `glibc-2.18`. However, this fix was not classified as a security problem, and as a result, many stable and long-term-support distributions remain vulnerable.

Linux systems that are liable to attack include Debian 7 (Wheezy), RHEL 5, 6, and 7, CentOS 6 and 7 and Ubuntu 12.04.

Various product vendors are rolling out updates to patch their affected distributions. We strongly recommend that you check with your Linux distribution vendor to see if they have a patch available. If so, you should review how to apply this patch to your environment as soon as possible in order to mitigate potential risk, as the bug is deemed critical.

Clavister's products are not affected by this vulnerability.

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