Does the GHOST vulnerability affect any Globalscape products?

THE INFORMATION IN THIS ARTICLE APPLIES TO:

- All Globalscape products

QUESTION

Does the "GHOST" vulnerability affect any Globalscape products?

ANSWER

No, as long as the system on which our product is installed is patched against the vulnerability.

MORE INFORMATION

On 27 January 2015, the United States Department of Homeland Security, via its Computer Emergency Readiness Team (US-CERT), warned organizations about a critical software vulnerability dubbed as “GHOST” that poses a serious risk to computer systems. “GHOST” affects Linux GNU C Library (glibc) versions prior to 2.18. Hackers can exploit this vulnerability via a remote code execution, which can enable them to take control over the affected system and wreak havoc by potentially deleting files, installing malware, and any other activity that can be done via stolen credentials.

Any Linux system running a vulnerable version of the glibc should be patched.

Refer to
https://www.us-cert.gov/ncas/current-activity/2015/01/27/Linux-Ghost-Remote-Code-Execution-Vulnerabi
for more information.

GlobalSCAPE Knowledge Base
https://kb.globalscape.com/Knowledgebase/11193/Does-the-GHOST-vulnerability...