NVD DB Update

CVE-2017-17562 - Score: 8.1

Components:

embedthis goahead *

Description:

Embedthis GoAhead before 3.6.5 allows remote code execution if CGI is enabled and a CGI program is dynamically linked. This is a result of initializing the environment of forked CGI scripts using untrusted HTTP request parameters in the cgiHandler function in cgi.c. When combined with the glibc dynamic linker, this behaviour can be abused for remote code execution using special parameter names such as LD_PRELOAD. An attacker can POST their shared object payload in the body of the request, and reference it using /proc/self/fd/0.

Main problems:

-1 no CWE Description available

https://cybersword.tech
ph1sher
www.linkedin.com/in/cybersword-tech
@davidwowa