预警编号：YJ-2017036

恒安嘉新

GoAhead Web Server 存在

远程代码执行漏洞

安全预警通告

恒安嘉新（北京）科技股份公司

2017 年 12 月 19 日

1 漏洞描述

近期，互联网爆出 GoAhead Web Server 远程代码执行漏洞（CVE-2017-17562），攻击者可利用上述漏洞使用特殊的参数名称如 LD_PRELOAD 劫持 libc 库，从而导致远程代码执行。漏洞危害程度为高危(High)。

2 影响范围

该漏洞会影响 GoAhead 2.5.0～3.6.5（不含 3.6.5）之间的所有版本。（GoAhead 2.5.0 版本开始进行了重构，之前的版本在网上已不可寻）

3 漏洞原理

GoAhead 是一个开源(商业许可)、简单、轻巧、功能强大、可以在多个平台运行的嵌入式 Web Server。它是世界上最受欢迎的嵌入式 Web 服务器，被部署在数以百万计的嵌入式设备上。

近日，GoAhead 被曝出远程命令执行漏洞。该漏洞源于使用不受信任的 HTTP 请求参数初始化 CGI 脚本环境，并且会影响所有启用了动态链接可执行文件（CGI 脚本）支持的用户。当与 glibc 动态链接器结合使用时，使用特殊变量（如 LD_PRELOAD）可以滥用该漏洞，从而导致远程代码执行。

4 修复建议

GoAhead 官方已发布安全更新公告，并发布了最新版 3.6.5 对该漏洞进行了修复。恒安嘉新强烈建议受影响的用户尽快升级到最新版本进行防护：https://github.com/embedthis/goahead/releases。