

What is Shellshock?

Shellshock is the name for CVE-2014-6271 and follow-up bugs in GNU Bash through version 4.3, disclosed on September 24, 2014. Bash imported function definitions from environment variables and also ran any commands placed after the definition, so a variable like `() { ;; }; /bin/id` executed `id` as soon as Bash started. Web servers using CGI copy request headers into environment variables, so a single crafted User-Agent header gave remote code execution. Patched Bash releases closed it; the CVSS score was 10.0.

HOW IT WORKS

01 How the attack works and how to test

Shown for defensive context:

- Local test: `env x='() { :; }; echo vulnerable' bash -c "echo test"`. A patched Bash prints only `test`; a vulnerable one prints `vulnerable` first.
- Remote CGI attack: a request to a CGI script with a header such as `User-Agent: () { :; }; /bin/bash -c 'id'`. The server copies the header into an environment variable, starts Bash to run the script and executes the appended command.
- What followed in 2014: botnets scanned the internet for `/cgi-bin/` paths within hours, dropping malware and opening reverse shells.

Shellshock still turns up in old embedded devices, appliances and forgotten CGI scripts during internal penetration tests.

HOW TO DEFEND

- Patch Bash through your operating system vendor. Any supported distribution has carried fixed Bash for years; the risk now lives in unpatched appliances, IoT devices and end-of-life systems.
- Retire CGI where you can, and never let CGI scripts run through Bash with request data in the environment.
- Inventory embedded devices with web interfaces, since many ran Bash or a vulnerable shell and never received updates.
- Hunt for `() {` in web server logs, which is the signature of Shellshock probes.

SOURCES

- [1] NVD: CVE-2014-6271
- [2] MITRE CWE-78: OS Command Injection
- [3] CISA Known Exploited Vulnerabilities Catalog
- [4] MITRE ATT&CK: Exploit Public-Facing Application (T1190)

Find the path to a shell before an attacker does.

securelayer7.net/learn/web-exploitation/what-is-shellshock

[Open online](https://securelayer7.net/learn/web-exploitation/what-is-shellshock)