COMET

Competence Centers for
Excellent Technologies

secure
sba-research.org

# Shellshock a.k.a. Bashbleed

| | |
|---|---|
| **Version** | 1.1 |
| **Datum** | 29. September 2014 |
| **Kontakt** | bashbleed@sba-research.org |

secure
sba-research.org

bmvit Bundesministerium für Verkehr, Innovation und Technologie

bmwfj Bundesministerium für Wirtschaft, Familie und Jugend

Christian Doppler Forschungsgesellschaft

FFG

wirtschaftsagentur wien

zit Die Technologieagentur der Stadt Wien

## Was ist Shellshock?

Am 24.9.2014 wurde eine Sicherheitsschwachstelle als CVE-2014-6271 (auch Shellshock oder Bashbleed) veröffentlicht. Die Sicherheitslücke befindet sich in der Kommandozeilensoftware bash, die praktisch in allen Linux-Systemen als Standard-Shell eingesetzt wird. Durch einen Fehler beim Parsen von Umgebungsvariablen wird das Ausführen von beliebigen Befehlen möglich. Die Schwachstelle lässt sich unter bestimmten Umständen auch von extern über das Internet ausnutzen und wird mit Stand 29.9.2014 auch bereits durch externe Angreifer aktiv ausgenutzt.

## Auswirkungen

Das gefährliche ist, dass bash an vielen Stellen implizit verwendet wird, wodurch externe Angriffsmöglichkeiten über das Internet existieren. Am einfachsten lässt sich diese Schwachstelle durch Angriffe über Webserver, die CGI-Skripte anbieten, praktisch ausnutzen. Das Ausführen von CGI-Skripten beinhaltet nämlich einen Aufruf der bash, bei der Benutzereingaben als Umgebungsvariablen mitgeschleust werden. **Dadurch ist es einem Angreifer unter bestimmten Umständen möglich, eigene Kommandos auf dem verwundbaren Webserver auszuführen und somit den Webserver zu übernehmen!** Dies passiert auch bereits im Rahmen automatisierter Attacken wie die Beobachtungen auf Honeypotsystemen zeigen.

## Überprüfung

Nur ein direkter Zugriff auf das System erlaubt eine verlässliche Überprüfung, ob man betroffen ist. Dazu geben Sie folgende Zeile in der Shell ein:

```
env x='() { :;}; echo vulnerable' bash -c "echo this is a test"
```

Wenn der String „vulnerable“ ausgegeben wird, ist eine verwundbare Version des Programms bash im Einsatz.

Wenn die Anzahl an Systemen unüberschaubar ist, empfehlen wir folgende Vorgangsweise, um die kritischsten Systeme zuerst zu sichern:

1. Welche extern erreichbaren Linux-Systeme habe ich?
2. Welche davon bieten CGI-Skripte an?

## Behebung

Alle namenhaften Linux-Distributionen bieten über ihre Betriebssystem-Update-Kanäle Updates für das bash-Paket an, die die Schwachstelle beheben. Während die ersten Patches unvollständig waren, gibt es mittlerweile bei allen Distributionen eine zweite Runde an Updates, die die Schwachstelle tatsächlich behebt.. **Wir empfehlen daher dringend die Bash-Pakete auf ihre Aktualität zu prüfen!**

## Kontakt

Für nähere Informationen oder Unterstützung bei der Überprüfung wenden Sie sich bitte an:

bashbleed@sba-research.org

SBA Research gGmbH
www.sba-research.org