COMET

Competence Centers for
Excellent Technologies

secure
sba-research.org

Shellshock a.k.a. Bashbleed

Version	1.0
Datum	25. 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 einem externen Angreifer ausnutzen.

Auswirkungen

Das gefährliche ist, dass bash an vielen Stellen implizit verwendet wird, wodurch externe Angriffsmöglichkeiten über das Internet existieren. Am offensichtlichsten erscheinen Angriffe über Webserver, die CGI-Skripte anbieten. Das Ausführen von CGI-Skripten beinhaltet 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!** Über weitere Angriffsvektoren informieren in den nächsten Versionen dieses Statements.

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

Die meisten Distributionen bieten über ihre Betriebssystem-Update-Kanäle bereits Updates für das bash-Paket an, das die Schwachstelle behebt. Es finden derzeit allerdings noch Diskussionen statt, ob die derzeitige Behebung wirklich alle Angriffe abdeckt. **Wir empfehlen dennoch bereits jetzt ein Update durchzuführen, da es jedenfalls die derzeit bekannten Angriffsmuster verhindert!**

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