

Shellshock

With all details

Proseminar - Aktuelle IT-Sicherheitsvorfälle und Lösungsansätze

Martin Weiss, Kay Schmitteckert | 16. Dezember 2015

FORSCHUNGSGRUPPE DEZENTRALE SYSTEME UND NETZDIENSTE - TM & SCC



- 1 Shellshock
- 2 Hätte man Shellshock vorbeugen können?
- 3 Präventive Verteidigungsmaßnahmen
- 4 Maßnahmen gegen SQL-Injections
- 5 Fazit und Resümee

Was ist Shellshock?

- Bash Sicherheitslücke
- Entdeckung September 2014
- Existiert seit 1989
- CVE-Nummern CVE-2014-6271, -7169, -7168, -7187, -6277, -6278
- 3 Patches bis zur Behebung

Was ist Shellshock?

- Bash Sicherheitslücke
- Entdeckung September 2014
- Existiert seit 1989
- CVE-Nummern CVE-2014-6271, -7169, -7168, -7187, -6277, -6278
- 3 Patches bis zur Behebung

Was ist Shellshock?

- Bash Sicherheitslücke
- Entdeckung September 2014
- Existiert seit 1989
- CVE-Nummern CVE-2014-6271, -7169, -7168, -7187, -6277, -6278
- 3 Patches bis zur Behebung

Was ist Shellshock?

- Bash Sicherheitslücke
- Entdeckung September 2014
- Existiert seit 1989
- CVE-Nummern CVE-2014-6271, -7169, -7168, -7187, -6277, -6278
- 3 Patches bis zur Behebung

Was ist Shellshock?

- Bash Sicherheitslücke
- Entdeckung September 2014
- Existiert seit 1989
- CVE-Nummern CVE-2014-6271, -7169, -7168, -7187, -6277, -6278
- 3 Patches bis zur Behebung

Ausmaß des Exploits

- Bash Standard-Shell bei vielen unixoiden Systemen
- Großteil der Webserver laufen unter unixoiden Systemen
- Weltweit waren hunderte Millionen Computer betroffen
 - Unter anderem Server von Yahoo, Winzip und Lycos
- Forscher halten die Sicherheitslücke für gravierender als Heartbleed

Ausmaß des Exploits

- Bash Standard-Shell bei vielen unixoiden Systemen
- Großteil der Webserver laufen unter unixoiden Systemen
- Weltweit waren hunderte Millionen Computer betroffen
 - Unter anderem Server von Yahoo, Winzip und Lycos
- Forscher halten die Sicherheitslücke für gravierender als Heartbleed

Ausmaß des Exploits

- Bash Standard-Shell bei vielen unixoiden Systemen
- Großteil der Webserver laufen unter unixoiden Systemen
- Weltweit waren hunderte Millionen Computer betroffen
 - Unter anderem Server von Yahoo, Winzip und Lycos
- Forscher halten die Sicherheitslücke für gravierender als Heartbleed

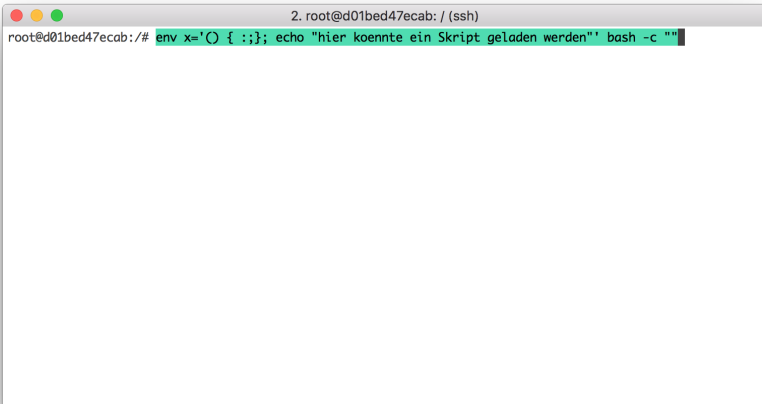
Ausmaß des Exploits

- Bash Standard-Shell bei vielen unixoiden Systemen
- Großteil der Webserver laufen unter unixoiden Systemen
- Weltweit waren hunderte Millionen Computer betroffen
 - Unter anderem Server von Yahoo, Winzip und Lycos
- Forscher halten die Sicherheitslücke für gravierender als Heartbleed

Ausmaß des Exploits

- Bash Standard-Shell bei vielen unixoiden Systemen
- Großteil der Webserver laufen unter unixoiden Systemen
- Weltweit waren hunderte Millionen Computer betroffen
 - Unter anderem Server von Yahoo, Winzip und Lycos
- Forscher halten die Sicherheitslücke für gravierender als Heartbleed

Ungepatchte Bash



A terminal window titled "2. root@d01bed47ecab: / (ssh)" showing a root prompt. The command entered is `env x='() { :; }; echo "hier koennte ein Skript geladen werden"' bash -c ""`, which is highlighted in green. The command is a Shellshock exploit designed to load a script.

Ungepatchte Bash

```
2. root@d01bed47ecab: / (ssh)
root@d01bed47ecab:/# env x='()' { :;}; echo "hier koennte ein Skript geladen werden" bash -c ""
hier koennte ein Skript geladen werden
root@d01bed47ecab:/#
```

Ja!

Möglichkeiten

- Präventive Verteidigungsmaßnahmen

- Maßnahmen gegen SQL-Injections

Möglichkeiten

- Präventive Verteidigungsmaßnahmen

- Maßnahmen gegen SQL-Injections

Möglichkeiten

- Präventive Verteidigungsmaßnahmen
- Maßnahmen gegen SQL-Injections

Mehrschichtige Sicherheitsstrukturen

- Experten: Sicherheitslücken nicht zu 100% ausschließbar
- Können aber durch mehrschichtige Sicherheitsstrukturen migriert werden
- Torvalds: „The only real solution to security is to admit that bugs happen, and then mitigate them by having multiple layers, so if you have a hole in one component, the next layer will catch the issue.“

Mehrschichtige Sicherheitsstrukturen

- Experten: Sicherheitslücken nicht zu 100% ausschließbar
- Können aber durch mehrschichtige Sicherheitsstrukturen migriert werden
- Torvalds: „The only real solution to security is to admit that bugs happen, and then mitigate them by having multiple layers, so if you have a hole in one component, the next layer will catch the issue.“

Mehrschichtige Sicherheitsstrukturen

- Experten: Sicherheitslücken nicht zu 100% ausschließbar
- Können aber durch mehrschichtige Sicherheitsstrukturen migriert werden
- Torvalds: „The only real solution to security is to admit that bugs happen, and then mitigate them by having multiple layers, so if you have a hole in one component, the next layer will catch the issue.“

Zugriffskontrolle

- Zugriffskontrolle kann eine Schicht sein
- Zentrale Frage: Wer darf auf welche Daten lesen, schreiben, ausführen?
- Drei grundlegende Modelle:
 - Mandatory Access Control (MAC)
 - Discretionary Access Control (DAC)
 - Role-based Access Control (RBAC)

Zugriffskontrolle

- Zugriffskontrolle kann eine Schicht sein
- Zentrale Frage: Wer darf auf welche Daten lesen, schreiben, ausführen?
- Drei grundlegende Modelle:
 - Mandatory Access Control (MAC)
 - Discretionary Access Control (DAC)
 - Role-based Access Control (RBAC)

Zugriffskontrolle

- Zugriffskontrolle kann eine Schicht sein
- Zentrale Frage: Wer darf auf welche Daten lesen, schreiben, ausführen?
- Drei grundlegende Modelle:
 - Mandatory Access Control (MAC)
 - Discretionary Access Control (DAC)
 - Role-based Access Control (RBAC)

Zugriffskontrolle

- Zugriffskontrolle kann eine Schicht sein
- Zentrale Frage: Wer darf auf welche Daten lesen, schreiben, ausführen?
- Drei grundlegende Modelle:
 - Mandatory Access Control (MAC)
 - Discretionary Access Control (DAC)
 - Role-based Access Control (RBAC)

Zugriffskontrolle

- Zugriffskontrolle kann eine Schicht sein
- Zentrale Frage: Wer darf auf welche Daten lesen, schreiben, ausführen?
- Drei grundlegende Modelle:
 - Mandatory Access Control (MAC)
 - Discretionary Access Control (DAC)
 - Role-based Access Control (RBAC)

Zugriffskontrolle

- Zugriffskontrolle kann eine Schicht sein
- Zentrale Frage: Wer darf auf welche Daten lesen, schreiben, ausführen?
- Drei grundlegende Modelle:
 - Mandatory Access Control (MAC)
 - Discretionary Access Control (DAC)
 - Role-based Access Control (RBAC)

Sandboxing

- blablabla...

AppArmor

- Einfache Umsetzung von Mandatory Access Control (MAC)
- Schränkt die Rechte von Applikationen ein
- Im Vergleich zu SELinux einfache Konfiguration

AppArmor

- Einfache Umsetzung von Mandatory Access Control (MAC)
- Schränkt die Rechte von Applikationen ein
- Im Vergleich zu SELinux einfache Konfiguration

AppArmor

- Einfache Umsetzung von Mandatory Access Control (MAC)
- Schränkt die Rechte von Applikationen ein
- Im Vergleich zu SELinux einfache Konfiguration

Docker

■ blabla...

Vergleich AppArmor & Docker

- blabla...

Fazit

- blabla...

Möglichkeiten

- Präventive Verteidigungsmaßnahmen
- Maßnahmen gegen SQL-Injections
- ...

Möglichkeiten

- Präventive Verteidigungsmaßnahmen
- Maßnahmen gegen SQL-Injections
- ...

Möglichkeiten

- Präventive Verteidigungsmaßnahmen

- Maßnahmen gegen SQL-Injections

Möglichkeiten

- Präventive Verteidigungsmaßnahmen

- Maßnahmen gegen SQL-Injections

Möglichkeiten

- Präventive Verteidigungsmaßnahmen
- Maßnahmen gegen SQL-Injections