Karlsruher Institut für Technologie

Shellshock
With all details

Proseminar - Aktuelle IT-Sicherheitsvorfälle und Lösungsansätze

Martin Weiss, Kay Schmitteckert | 15. Dezember 2015

FORSCHUNGSGRUPPE DEZENTRALE SYSTEME UND NETZDIENSTE - TM & SCC

Agenda

Shellshock

Was ist Shellshock?

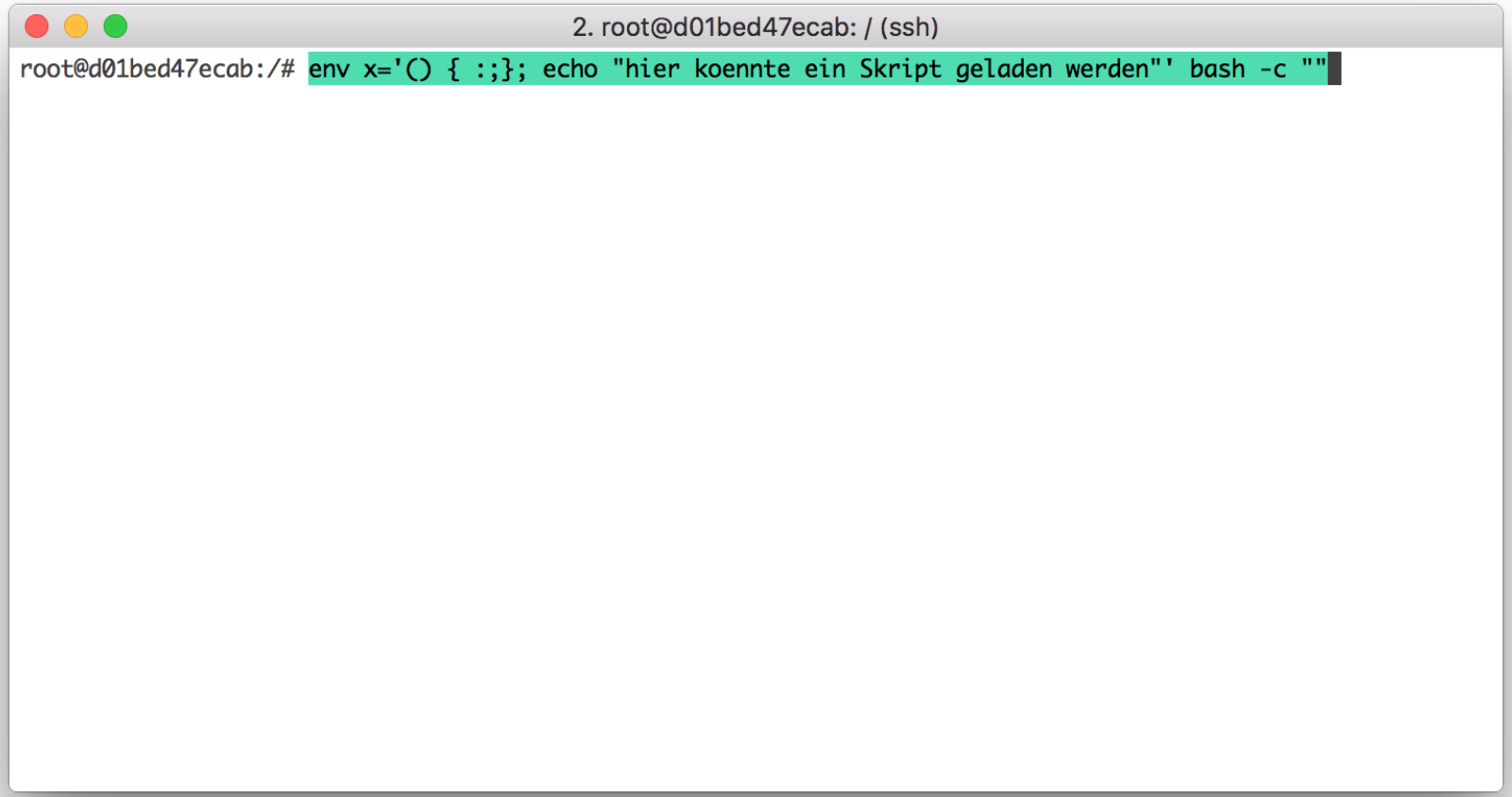
- Bash Sicherheitslücke
- Entdeckung September 2014
- Existiert seit 1989
- CVE-Nummern CVE-2014-6271, -7169, -7168, -7187, -6277, -6278
- 3 Patches bis zur Behebung

Shellshock

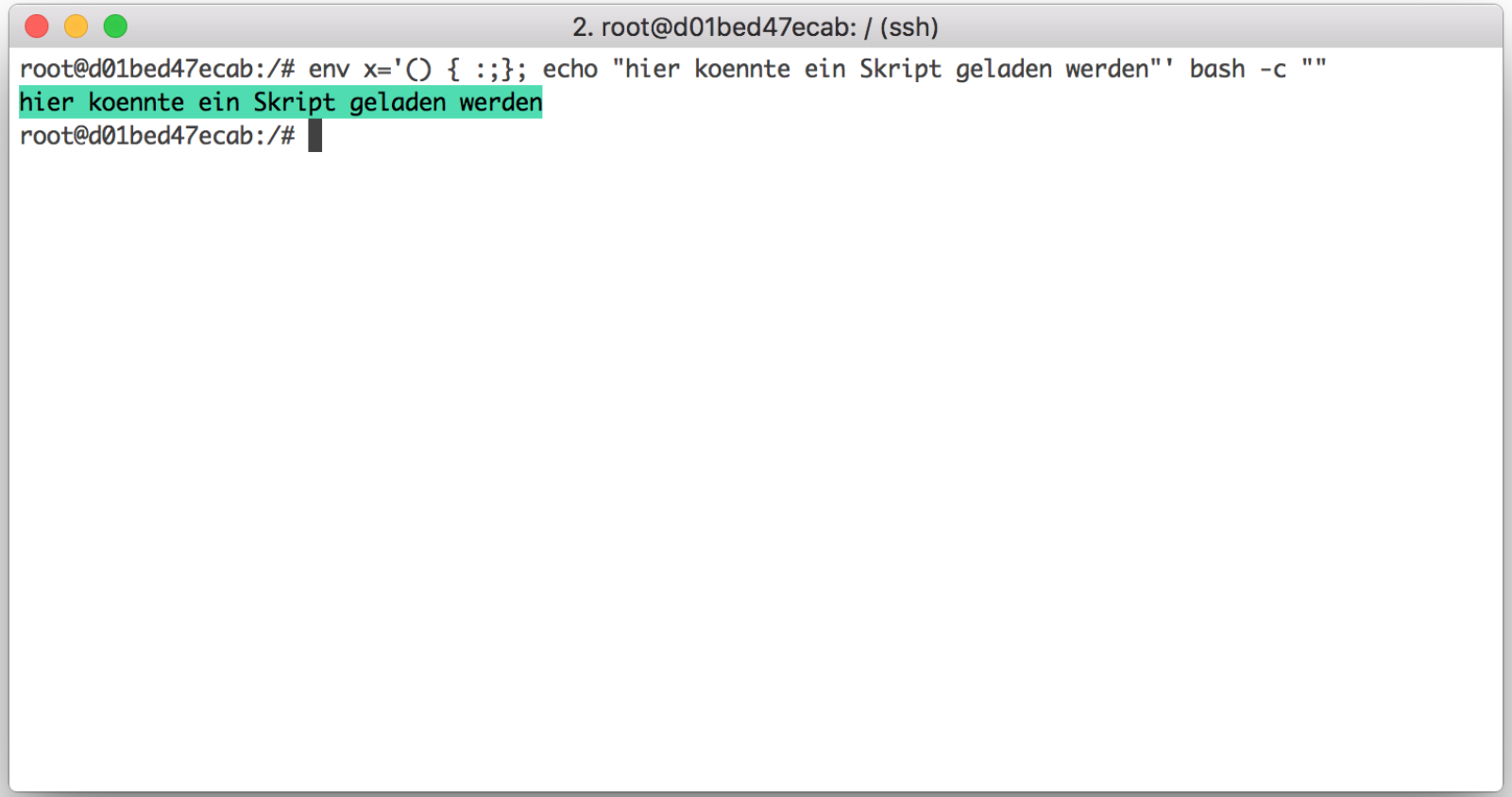
Ausmaß des Exploits

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

Ungepatchte Bash



Ungepatchte Bash



Vorbeugung von Shellshock möglich?

Ja!

Vorbeugung von Shellshock möglich?

Möglichkeiten

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

Vorbeugung von Shellshock möglich?

Möglichkeiten

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

Präventive Verteidigungsmaßnahmen

Example 1

- Bullet point 1
- Bullet point 2
- ...

Präventive Verteidigungsmaßnahmen

Example 1

- Bullet point 1
- Bullet point 2
- ...

Example slide D

Alert 1

- Bullet point 1
- Bullet point 2
- . . .

Example slide D

Alert 1

- Bullet point 1
- Bullet point 2
- . . .

Präventive Verteidigungsmaßnahmen

Möglichkeiten

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

Präventive Verteidigungsmaßnahmen

Möglichkeiten

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

Maßnahmen gegen SQL-Injections

Möglichkeiten

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

Maßnahmen gegen SQL-Injections

Möglichkeiten

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

Fazit und Resümee

Möglichkeiten

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

Fazit und Resümee

Möglichkeiten

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