

Debian GNU/Linux

安全合规之路

杨旭

Day Job: 广州市腾御安信息科技有限公司

职位: 基础架构安全运维

Night Job: HardenedLinux 社区成员

Github: github.com/n3o4po11o/

Mail: n3o4po11o@gmail.com



HardenedLinux

Why Debian ?



debian

- 众多的开发者
- 持续更新
- 良好的生态

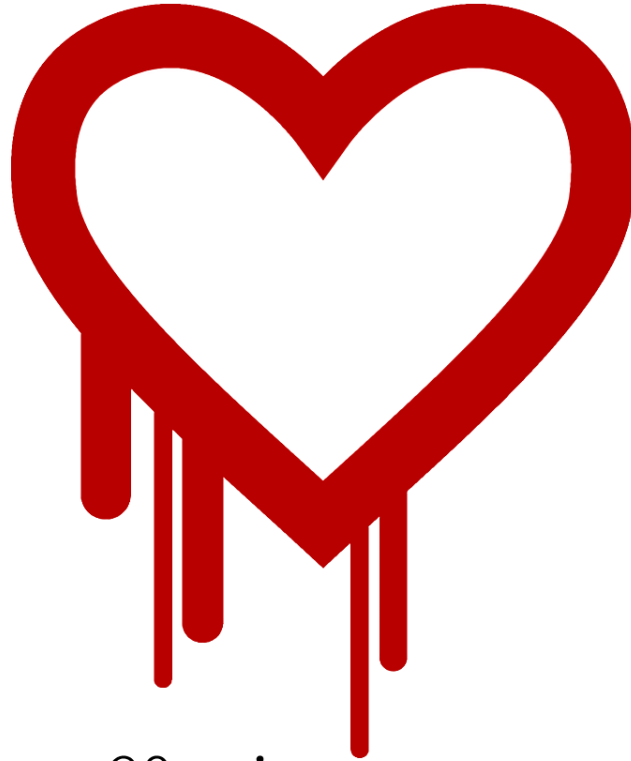


debian

- 众多的开发者
- 持续更新
- 良好的生态



Heartbleed



Fixing time: less than 30 mins



debian

- 众多的开发者
- 持续更新
- 良好的生态



Kernel

Debian Kernel maintainers: Ben Hutchings

Linux 3.2 kernel: since 2012-01-04

Frequency(avg): 2 fix a day, 2 weeks a release



Kernel

“If you are not using a stable/longterm kernel, your machine is insecure”

– Grey Kroah-Hartman



Kernel

“Debian is doing a awesome job. So a non-profit organization built volunteer people is doing a better job than some largest Linux provider. That"s a shame. ”

– Grey Kroah–Hartman



Kernel

“Base you software on Debian, or update your kernel on time”

– Grey Kroah–Hartman



debian

- 众多的开发者
- 持续更新
- 良好的生态

Mempo

ReproducibleBuilds

MEMPO



TAKE ACTION NOW
Oppose NSA Mass Spying!

NSA image from eff.org

Mempo image from debian.org

Military

&

Intelligence

ASTRA LINUX

Linux 4.2 kernel

PaX kernel patch

Non-standard MAC

俄罗斯国密GOST

Military
&
Intelligence



CLIP



推动debian安全合规可能的选择

The Deepin logo, consisting of the word "deepin" in a white, lowercase, sans-serif font, centered on a solid teal square background.

deepin

1. Debian 系
2. "国产" GNU/Linux操作系统中最靠谱的厂商

Compliance?

STIG ?

RHEL

STIG

Security Technical Implementation Guides (STIGs)

RHEL

STIG



redhat®



**BIG
BROTHER
IS
WATCHING**

严重等级

- | | |
|---------|---------------------------------|
| CAT I | 对不合理配置的利用会直接并立即影响设备的机密性、可用性和完整性 |
| CAT II | 对不合理配置的利用可能影响设备的机密性、可用性和完整性 |
| CAT III | 存在不合理的配置会降低对设备机密性、可用性和完整性的保护 |

CAT I

in RHEL 6 V1R7 STIG

unsecure services: rsh, rexec, telnet, rlogin, ssh v1

secure package: check gpg key, no signature packages

data security: check insecure_locks

weak password: ssh, system-auth

CAT II

in RHEL 6 V1R7 STIG

check owner, group owner, group member, permissions:
gshadow, passwd, shadow, group, audit, /lib(64),
/usr/lib(64), (default System binaries), rsyslog_log
check firewall: ip(6)tables default policy, ipv4_forward,
enforce password: min-length, max expired day,
changing frequency

CAT II

in RHEL 6 V1R7 STIG

system authentication related: hash, uid, faillock
others: check mail systems, tuning auditd(disk_errors,
disk_full, etc), ssh lastlog, backup mechanism(OS, USER,
auditd_log), enforce connection of mobile devices

CAT III

in RHEL 6 V1R7 STIG

separate file system for: /var, /tmp, /var/log/audit,
/home/\$USER,

account related: PASS_WARN_AGE, pam_cracklib
(dcredit, maxrepeat, uppercase/lowercase alphabetic,
special character, difok, maxrepeat), expiration day,
INACTIVE


CAT III

in RHEL 6 V1R7 STIG

kernel tuning: martian packet, ICMP

auditd: attempts to alter system time, account,
network, MAC, DAC, access files, setuid/setgid, file
system mounts, files deletions, /etc/sudoers,

others: cryptographically verify package, LUKS enable,
ClientAliveInterval/ClientAliveCountMax/PermitUserEnvir
onment



STIG-4-Debian

项目地址：<https://github.com/hardenedlinux/STIG-4-Debian>

第一版完成时间：28/06/2015





自由软件社区生态
&
立法的生态

Kernel

Firmware

密码工程

Compiler

GNU/Linux 安全体系

基于自由软件的场景化加固

ONCE, THERE WERE SEVEN KINGDOMS . . .
C. 2 YEARS BEFORE CONQUEST

Thank to:

Pax/Grsecurity Community

Debian Community

RHEL STIG

Shawn C[a.k.a "citypw"]