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



Why Debian?



- 众多的开发者
- 持续更新

debian · 良好的生态



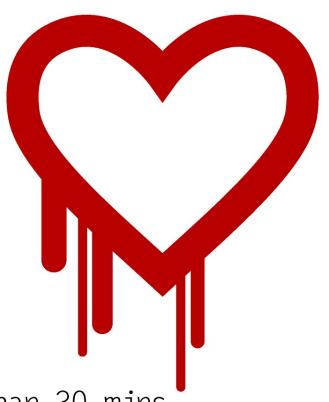
• 众多的开发者

• 持续更新

debian · 良好的生态



Heartbleed



Fixing time: less than 30 mins



- 众多的开发者
- 持续更新

debian · 良好的生态



Debian Kernel maintainers: Ben Hutchings

Linux 3.2 kernel: since 2012-01-04

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



"If you are not using a stable/longterm kernel, you machine is insecure"

Greg Kroah-Hartman



"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."

- Greg Kroah-Hartman



"Base you software on Debian, or update your kernel on time"

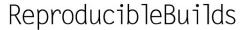
- Greg Kroah-Hartman



- 众多的开发者
- 持续更新

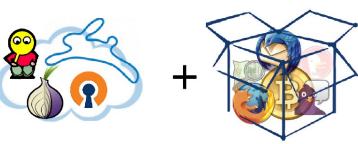
debian · 良好的生态

Mempo











Military & Intelligence



Linux 4.2 kernel

PaX kernel patch

Non-standard MAC

俄罗斯国密GOST

Military & Intelligence



Compliance?

STIG?

STIG

Security Technical Implementation Guides (STIGs)

STIG







RHEL

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、				

RHEL STIG

in RHEL 7 V1R1 STIG

check package: package hash/screen/rsh-server/ypserv/(t)ftp

check: password quality/password mechanism/cipher (PAM/ssh/Grub)

check configuration/rules: (ssh/auditd/sysctl)

check file: owner/group owner/permission

check services: automounter/Apparmor/(r)syslog

check operation system: supported release/graphical interface

and so on...

STIG-4-Debian

基于Bash shell 支持html模板输出 检测单元"模块化"

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

第一版完成时间: 28/06/2015 (For Debian 8)

第二版完成时间: 19/09/2017 (For Debian 9)

STIG for Debian 9 checking report

Date: 2017-09-21

Automatic checking		Pass count: 49	Failed count: 139	(Click for more details)	
Rule ID	Rule Title			Severity	Status
SV- 86479r2_rule	The cryptogra	aphic hash of system file	es and commands must match vendor	high	FAILED
SV- 86521r1_rule	The operating	g system must have the	screen package installed.	medium	FAILED
SV- 86527r2_rule	-	ords are changed or nev st contain at least one u	v passwords are established, the new apper-case character.	medium	FAILED
SV- 86529r2_rule	-	ords are changed or nev st contain at least one lo	medium	FAILED	
SV- 86531r2_rule		ords are changed or nev st contain at least one n	medium	FAILED	
SV- 86533r1 rule	-	ords are changed or nev st contain at least one s	medium	FAILED	

https://github.com/hardenedlinux/Debian-GNU-Linux-Profiles

DNS

Basic bind9 configuration for lan Deploy Bro as an IDS

Domain based routing on openwrt

HA

Using UPS with NUT

IDS

Storage

Manually deploy ceph cluster step

by step

https://github.com/hardenedlinux/Debian-GNU-Linux-Profiles

Harbian QA

IPSEC

Benchmarking PaX/Grsecurity kernel Building IPSEC VPN via strongswan

on Debian GNU/Linux

MAC/RBAC

Syzkaller crash DEMO

Grsecurity RBAC system with nginx

Kernel QA with syzkaller and qemu

practice

https://github.com/hardenedlinux/Debian-GNU-Linux-Profiles

Hardened boot

Ways to build your own trustchain for secureboot

Debian Hardened boot

Grub for Coreboot/Grub for Secure boot

Preparation for Secure Boot on Key Management Server

Set Up Unrestricted Secure Boot On supporting machine

https://github.com/hardenedlinux/Debian-GNU-Linux-Profiles

SSH and Cluster

Powerful ssh(1) options you don't know

Ways to authenticate yourself to a remote virtual machine host

Recommended way to use ssh(1) for cluster management

https://github.com/hardenedlinux/Debian-GNU-Linux-Profiles

Security Operation Center

Using Logstash/Elasticsearch/Grafana to build a small SOC(Security Operation Center) from scratch

SOC Overview

https://github.com/hardenedlinux/Debian-GNU-Linux-Profiles

Unclassified

Small-scale Enterprise KVM Deployments With Kimchi
The recommended configs of host computers and management
console running Debian GNU/Linux within clusters

https://github.com/hardenedlinux/Debian-GNU-Linux-Profiles

TLS

TLS Mutual Authentication in Webday

TLS Mutual Authentication in Gitlab

OpenConnect Server For Anyconnect Compatible Service



Thank to:

Pax/Grsecurity Community

Debian Community

RHEL STIG

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