Debian Security Team presentation

Yves-Alexis Perez

SSTIC 2018

Introduction

Who am I?

Yves-Alexis Perez (Corsac)

Debian developer

- **team security member**
- package maintainer
  - Xfce desktop environment
  - strongSwan IKE/IPsec daemon
  - Linux kernel team member

ANSSI head of software and hardware architecture lab

Mostly interested in low-level security and hardening

Agenda

Security team presentation

- People
- Roles
- Tools

Workflows

- Security frontdesk
- Debian Security Advisory

Vulnerabilities

- Embargos

Examples

- KRACK
- Meltdown/Spectre
- Standard embargoed vulnerability: pcs

Security team presentation

People

Core team members

- ~10 people[1]
- ~5 really active

Other people involved

- Debian developers and maintainers
- Security researchers

What we do

Handle security for stable releases

- keep watch over security issues in stable/oldstable
- issue Debian Security Advisories (DSA)
  - prepare packages updates
  - upload to the security archive
  - send the DSA mail for debian-security-announce@
- coordinate with other teams and developpers

Other interests

- distribution hardening
  - reduces workload later on

What we don't do

Everything else security related

- Debian infrastructure: the *other* DSA[1]
- Debian accounts: DAM[2] and Keyring teams
- Debian LTS[3]

1. Debian System Administrators, unfortunate acronym collision
2. Debian Accounts Managers
3. Long Term Support

Frontends

Communication

- `security@debian.org` (PGP `rsa4096/0×6BAF400B05C3E651`)
- `debian-security-announce@lists.debian.org`
- `irc://irc.debian.org/#debian-security`

Security tracker: `https://security-tracker.debian.org/`

- sysadmin/enduser oriented
- web interface for browsing
- search by package, vulnerability (CVE) or suite

Data: useful for automated vulnerability assessment

- CVE list (raw[2] / json[3])
- OVAL json [4]

Backends

security-tracker

Public[5] git repository

- team organization
- CVE management
- DSA assignment
- source for security-tracker website

sec-private

Private git repository

- management of embargoed issues
- some internal data

Workflows

Security frontdesk

Contact point for security issues

Make sure:

- someone is always present and active
- we don't miss important issues
- we distribute the load amongst the team

- *Anyone* can do this, but make sure *someone* actually does it
- nowadays not formally done

Duties

Day to day routine

- watch over the mail alias and process incoming requests
- watch over oss-sec and distros (private) lists, external sources
- add private issues to the private git repository
- add public issues to the security-tracker (`data/CVE/list`)
- process *External check*
- submit bug reports for public issues to the BTS
- add new DSA-worthy issues to the list (`dsa-needed.txt`)

Distributed amongst the team

External check

What is it?

- automated script
- runs once a day
- finds newly assigned CVEs from various sources MITRE, vendors/upstream etc.
- adds them to `data/CVE/list` with TODO tag

Post processing TODO entries

- is it against a Debian package?
- is the affected version in a Debian supported release?
- what is the severity?
- are there external sources of information?

Add enough information to the tracker to facilitate work later on

Releasing a DSA[6]

1. vulnerability is identified
2. CVE is assigned (helpful, not required)
3. fix is identified
4. patch is applied against package in supported suites
5. package is built locally
6. package is uploaded to security-master
7. package is built by the buildbots
8. package is released to the security mirror network
9. DSA mail is sent

Usually

- work is shared between team members
- some steps can be done externally

Vulnerabilities

Three major types of vulnerability

public vulnerability (vast majority)

- reported via oss-sec, public bug or commit
- fix already known or developped in the open
- integrated in Debian as soon as possible
- usually no rush

simple private vulnerability

complex private vulnerability

- multiple codebases
- multiple vendors
- protocol vulnerability
- hardware vulnerability

Embargos

- vulnerability not known publically (*under embargo*)
- only small circle of people know about it

Usage

- give some time to developers to find a fix
- coordinated date for publication
- everybody publish at the same time
- all users protected

High profile examples

- ROCA (Debian not affected)
- KRACK (wpa)
- Meltdown/Spectre (Linux, hypervisors, microcode)

In practice

Embargos have many drawbacks

- fix availability delayed
- few people aware mean fix might not be optimal or even broken
- indefinite embargo problem (hide stuff below the carpet)
- leak problem

Limit usage as much as possible

- for simple vulnerabilities
- short duration

Operating system distribution security contact lists

`linux-distros@vs.openwall.org`[7]

- restricted list for open-source distributions (Linux and *BSD)
- successor to vendors-sec
- maintained by Openwall with help from distributions
- anyone can report a vulnerability privately
- strict policy (14 days max embargo, 7 days preferred)

Examples

KRACK

Standard embargoed vulnerability

- coordination with community (upstream, researchers...)
- fix preparation
- coordinated release

Key Reinstallation attacks[8]

- multiple vulnerabilities in the WPA *protocol*
- discovered by Mathy Vanhoef (imec-DistriNet, KU Leuven)
- involves multiple vendors (access points and clients)
- in Debian: wpa source package (wpa_supplicant and hostapd)

Timeline

28/08 initial contact from CERT

10/10 second contact from CERT

10/10 upstream contact on the restricted distribution list

10/10 contact wpa upstream and Debian maintainers

16/10 announcement and fixes publication

01/11 paper presentation at ACM CCS

Initial contact (28/08/2017)

[VU#793496] WPA2 protocol vulnerabilities

File Edit View Message

Reply Group Reply Forward

From: CERT Coordination Center <cert@cert.org>
To: Yves-Alexis <corsac@debian.org>, Debian Security Team <team@security.debian.org>
Cc: CERT Coordination Center <cert@cert.org>
Subject: [VU#793496] WPA2 protocol vulnerabilities
Date: Mon, 28 Aug 2017 11:39:25 -0400 (*28/08/2017 17:39:25*)
Security: GPG encrypted

Greetings,

We have become aware of several key management vulnerabilities in the 4-way handshake of the Wi-Fi Protected Access II (WPA2) security protocol. The impact of attacking these issues includes decryption, packet replay, TCP connection hijacking, HTTP content injection, and others. Note that as protocol-level issues, most or all correct implementations of the standard will be affected. Vendors who implement WPA2 are strongly encouraged to carefully review the attached report and proofs of concept.

The CERT/CC and the reporting researcher, Mathy Vanhoef (contact information below), will be publicly disclosing these issues on 16 October 2017. CERT welcomes and encourages your self-assessments and official statements for representation in our vulnerability note. Note that vendors we do not hear from will be listed as 'unknown' in our published document.

We are tracking this case as VU#793496. Please retain VU#793496 in the subject of any email replies.

Please note that this notification may be redundant to ICASI members. ICASI members have been working with the researcher to discuss fixes and compatibility issues under its member NDA. To enable collaboration across the community, ICASI welcomes the engagement of nonmembers into these discussions. For further information on how you can engage with ICASI on this, please contact Scott Algeier, ICASI's Executive Director, at scott@icasi.org or 703-385-4969.

You are also welcome to reach out to the researcher, Mathy Vanhoef <Mathy.Vanhoef@cs.kuleuven.be>, with technical questions about the vulnerabilities or proofs of concept. His PGP key may be found here:

http://pgp.mit.edu/pks/lookup?search=Mathy.Vanhoef%40cs.kuleuven.be&op=index

2 Attachments (885,6 kB) Save All

Initial contact (28/08/2017)

Summary

- coordination done by CERT.org
- full details, paper and proof of concept in the notification

Upstream contact (10/10/2017)

[vs] VU#228519 and wpa_supplicant/hostapd

File Edit View Message

Reply Group Reply Forward

From: Jouni Malinen <j@w1.fi>
To: distros@vs.openwall.org
Subject: [vs] VU#228519 and wpa_supplicant/hostapd
Date: Tue, 10 Oct 2017 23:08:56 +0300 (*10/10/2017 22:08:56*)
Security: GPG encrypted

plain text document attachment (msg-28317-2.txt)

```
VU#228519 (a generic issue related to reinstallation of IEEE 802.11
RSN/WPA keys) applies to a number of implementations including
wpa_supplicant and hostapd. The following security advisory will be
published October 16, 2017. This addresses the issues applicable to
wpa_supplicant/hostapd.

I'm providing this early notice to the distros list since hostapd and/or
wpa_supplicant packages are included in many of the distros on the list
and while some of you may have received information about this from
CERT, I'm not sure whether everyone has and there may be desire to
prepare for releasing updated packages in time the issues become public.

Please let me know if you have any feedback or questions regarding the
draft advisory or if you would like to receive the patches referenced at
the end of the document before the publication date.

- Jouni


---[ EMBARGO NOTE START ]------------------------------------------------
- This is an *UNPUBLISHED DRAFT* and subject to change
- Do *NOT* distribute any details outside your organization
```

1 Attachment (12,3 kB) Save As

Upstream contact (10/10/2017)

Summary

- from Jouni Malinen, upstream author of wpa
- sent to the distribution list (open-source distributions)
- details about the protocol vulnerabilities
- impact on hostapd and wpa_supplicant on various platforms
- patches for various branches
- later resent to oss-sec[9] (per distros list policy)

Embargo period

Investigate the issue

- read the announcements and the paper
- identify vulnerabilities relevant to hostapd/wpa_supplicant
- setup a testbed to reproduce the issues

Work with the maintainers

- integrate patches
- test-build packages for affected distributions (Sid/unstable, Stretch/stable, Jessie/oldstable)
- upload packages to security-master for buildds
- prepare advisory text

On release date

- small embargo break: Cisco and other vendors release early
- Web and Twitter start to panic
- Mathy Vanhoef publishes the website
- Distributions start sending mail
- Packages are released

Meltdown[10]

Reminder

- CVE-2017-5754 (Rogue Data Cache Load)
- affects all Intel CPU with out-of-order execution (nearly all since 95), some IBM POWER, some ARM CPU
- race condition between MMU permission checks and memory access
- invisible at the architecture level but visible at micro-architecture level
- exploited by measuring access time to memory whose location depends on privileged content
- reads data from any mapped memory, bypassing permission checks
- fixed by unmapping kernel from userland (KPTI[4])

4. Kernel Page-table Isolation

Spectre[11]

Reminder

- CVE-2017-5753 (bounds check bypass, Spectre-V1)
- CVE-2017-5715 (branch target injection, Spectre-V2)
- vulnerabilities in various CPU (Intel, ARM)
- root cause is speculative execution
- like Meltdown, attacker can read data normally not accessible at her privilege level (interpreter, CPL, hypervisor)
- fixed by combined hardware (or microcode) and software changes

Timeline

2016	multiple researches published on side-channel and cache timing attacks
2017	*Spectre attack vectors found by two separate teams*
01/06/2017	*Google researchers alert Intel, AMD, ARM about Spectre*
24/06/2017	Daniel Grass et al (TU Graz) publish “KASLR is Dead: Long Live KASLR” with KAISER patchset
28/07/2017	*Google alerts vendors about Meltdown*
09/2017	*Google internally deploys retpoline fix for Spectre*
11/2017	KAISER patchset is heavily discussed on LKML, fast-tracked for 4.15
09/11/2017	*Intel notifies some vendors under NDA (CRD 09/01/2018)*
12/2017	Rumors (Twitter etc.) of an incoming hardware vulnerability
03/01/2018	Google Project Zero publishes blog post, Spectre/Meltdown attack websites are up

Debian handling

Debian not included in embargo

- no NDA with Intel
- information only from the rumor mill
- lot of noise around KAISER/KPTI on early january
- on 03/01/2018
  - identify Meltdown and Spectre attack vectors
  - prioritize Meltdown fixes (KAISER for 4.9)
  - Spectre postponed (multiple incompatibles fixes, microcodes not released)
  - integrate kernel patches, build and test
- 04/01/2018: release kernel DSA fixing Meltdown

```
2018/01/03 - [16:56:46] (Corsac): but I keep
thinking an arbitrary read wouldn't lead to that
level of panic, and kind of fear there's a write
primitive somewhere too
```

pcs: pacemaker command-line interface

Two vulnerabilities

CVE-2018-1079 Privilege escalation via authorized user malicious REST call

CVE-2018-1086 Debug parameter removal bypass, allowing information disclosure

- discovered by a Red Hat researcher (Cedric Buissart)
- reported through distros@
- fixes already available
- CRD on 04/04/2018 (later extended to 09/04)
- Debian stable only affected by the information leak

Vulnerability handling

Timeline

- 26/03 initial contact to distros@ and acknowledgment
- 26/03 information forwarded to Debian maintainer
- 27/03 maintainer prepares update, tests the package
- 30/03 maintainer uploads the package
  package rejected because he's not a Debian developer
- 04/04 sponsor uploads to security-master
- 09/04 stable package released, DSA mail sent
- 12/04 new upstream version uploaded to unstable

Investigation

- simple vulnerability
- simple fix
- team work mostly coordination with maintainer
- embargo not necessarily needed but not harmful

Conclusion

What to bring home?

Security team

- handles security updates for (old)stable suites
- manages the security tracker

Not all vulnerabilities are equal

- public vs. private
- simple vs. complex
- isolated vs. multiple (cross-vendors, protocol etc.)

References

References

Debian, “Security team members.”
https://www.debian.org/intro/organization#security.

D. security team, “Cve list (raw).”
https://salsa.debian.org/security-tracker-team/security-tracker/raw/master/data/CVE/list.

D. security team, “Cve list (json).”
https://security-tracker.debian.org/tracker/data/json.

D. security team, “Oval data.”
https://www.debian.org/security/oval/.

D. security team, “Security tracker.”
https://salsa.debian.org/security-tracker-team/security-tracker.

D. security team, “Creation of a debian security advisory (full).”
https://wiki.debian.org/DebianSecurity/AdvisoryCreation/SecFull#.

Openwall, “Operating system distribution security contact lists.”
http://oss-security.openwall.org/wiki/mailing-lists/distros.

M. Vanhoef, “Key reinstallation attacks: Breaking wpa2 by forcing nonce reuse.”
https://www.krackattacks.com/.

J. Malinen, “wpa_supplicant/hostapd: Wpa packet number reuse with replayed messages and key reinstallation.”
http://www.openwall.com/lists/oss-security/2017/10/16/2.

M. Lipp, M. Schwarz, D. Gruss, T. Prescher, W. Haas, S. Mangard, P. Kocher, D. Genkin, Y. Yarom, and M. Hamburg, “Meltdown attack.”
http://meltdownattack.com/.

P. Kocher, D. Genkin, D. Gruss, W. Haas, M. Hamburg, M. Lipp, S. Mangard, T. Prescher, M. Schwarz, and Y. Yarom, “Spectre