Revue d'actualité de l'OSSIR

11 mai 2021

Aurélien Denis
*Vladimir Kolla @mynameisv_*

Failles / Bulletins / Advisories

Failles / Bulletins / Advisories (MMSBGA)
Microsoft

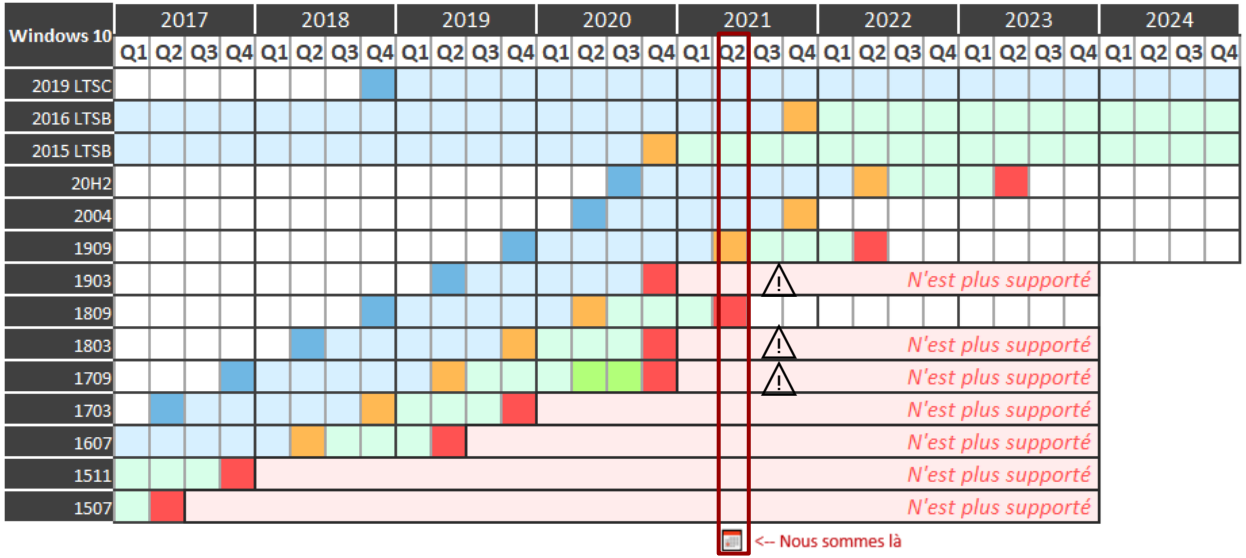
Report des fins de support de produits Microsoft suite au Covid-19

- Report de 6 mois
  - Windows 10, version 1709
  - Windows 10, version 1809
  - Windows Server, version 1809
  - Configuration Manager 1810
  - SharePoint Server 2010, SharePoint Foundation 2010, and Project Server 2010
  - Dynamics 365 cloud services
  - Basic Authentication in Exchange Online

https://www.bleepingcomputer.com/news/microsoft/microsoft-delays-end-of-support-for-older-windows-software-versions/

Failles / Bulletins / Advisories (MMSBGA)
Microsoft

Rappel du support Windows 10 en couleurs



mardi 13 novembre 2018	mardi 9 janvier 2024	mardi 9 janvier 2029
mardi 2 août 2016	mardi 12 octobre 2021	mardi 13 octobre 2026
mercredi 29 juillet 2015	mardi 13 octobre 2020	mardi 14 octobre 2025
mardi 20 octobre 2020	mardi 10 mai 2022	mardi 9 mai 2023
mercredi 27 mai 2020	mardi 14 décembre 2021	mardi 14 décembre 2021
mardi 12 novembre 2019	mardi 11 mai 2021	10 mai 2022**
mardi 21 mai 2019	mardi 8 décembre 2020	mardi 8 décembre 2020
mardi 13 novembre 2018	mardi 10 novembre 2020	11 mai 2021**
lundi 30 avril 2018	mardi 12 novembre 2019	mardi 10 novembre 2020
mardi 17 octobre 2017	~~9 avril~~ 4 sept. 2019	~~14 avril~~ 13 oct. 2020
5 avril 2017*	mardi 9 octobre 2018	mardi 8 octobre 2019
mardi 2 août 2016	mardi 10 avril 2018	mardi 9 avril 2019
mardi 10 novembre 2015	mardi 10 octobre 2017	mardi 10 octobre 2017
mercredi 29 juillet 2015	9 mai 2017	mardi 9 mai 2017

Légende :

- Date de mise à disposition pour le public et les entreprises
- Support
- Fin de support pour les versions Home, Pro, Pro Education et Pro for Workstations / fin de support standard pour LTSB/LTSC
- Support uniquement pour les versions Enterprise et Education
- Prolongation exceptionnelle suite au Coronavirus
- Fin de support pour toutes les versions / fin de support étendu pour LTSB/LTSC

Failles / Bulletins / Advisories
Microsoft - Avis

En avril :

- 108 vulnérabilités corrigées, dont 10 critiques

- A retenir :
  - CVE-2021-28480, CVE-2021-28481, CVE-2021-28482, CVE-2021-28483 (Exchange) *Made with ♡ by NSA*
  - CVE-2021-28310 : Exploitée in-the-wild

Composants impactés

Windows Server (2004) ;
Windows Server (1909) ;
Windows Server (20H2) ;
Windows Server 2008 ;
Windows Server 2012 ;
Windows Server 2016 ;
Windows Server 2019 ;
Windows 10 ;
Windows 7 ;
Windows 8.1 ;
Sharepoint ;
Microsoft 365 Apps ;
Microsoft Azure ;
Microsoft Office (Word, Excel, PowerPoint, Outlook) ;
Microsoft Edge ;
Microsoft Internet Explorer ;
Visual Studio ;
Windows Admin Center ;
Microsoft Visio.

Failles / Bulletins / Advisories
Microsoft - ProxyLogon (update)

Manipulation de données via une vulnérabilité au sein d'Exchange

- Drop de fichier arbitraire

  https://f5.pm/go-62102.html

(exploit) **Divulgation d'informations via une vulnérabilité au sein d'Exchange (CVE-2021-26855)**

- Récupération d'une boîte mail

  https://gitlab.com/gvillegas/ohwaa/

Failles / Bulletins / Advisories
CPU - Avril 2021

Oracle

- **390** correctifs de sécurité ont été publiés pour 30 produits.
- 30 vulnérabilités sont jugées critiques (score CVSS supérieur ou égal à 9.8).
- Correctifs à installer en priorité (RCE à distance sans authentification) :
  - Oracle Virtualization (CVE-2021-2177, CVE-2021-2248)
  - Oracle Systems (**CVE-2020-1472 (a.k.a. … ZeroLogon)**)
  - Oracle Storage Gateway (CVE-2021-2256, CVE-2021-2317)
- Infos techniques sur
  - CVE-2020-1472 (Oracle ZFS Storage)
  - CVE-2020-17530 (Oracle MySQL Enterprise Monitor) (Struts)
  - CVE-2019-17495 (Oracle Utilities Framework)
  - CVE-2019-17195 (Oracle Enterprise Manager Base Platform)

https://www.oracle.com/security-alerts/cpuapr2021.html

Produits impactés :

- Oracle Commerce
- Oracle Communications
- Oracle Communications Applications
- Oracle Construction and Engineering
- Oracle Database Server
- Oracle E-Business Suite
- Oracle Enterprise Manager
- Oracle Financial Services Applications
- Oracle Food and Beverage Applications
- Oracle Fusion Middleware
- Oracle Global Lifecycle Management
- Oracle Health Sciences Applications
- Oracle Hospitality Applications
- Oracle Hyperion
- Oracle iLearning
- Oracle Insurance Applications
- Oracle Java SE
- Oracle JD Edwards
- Oracle MySQL
- Oracle NoSQL Database
- Oracle PeopleSoft
- Oracle REST Data Services
- Oracle Retail Applications
- Oracle Siebel CRM
- Oracle Spatial Studio
- Oracle SQL Developer
- Oracle Storage Gateway
- Oracle Supply Chain
- Oracle Support Tools
- Oracle Systems
- Oracle Utilities Applications
- Oracle Virtualization

Failles / Bulletins / Advisories
Navigateurs (principales failles)

Manipulation de données et déni de service via 9 vulnérabilités au sein de Google Chrome

- Prises de contrôle du système
- Divulgation d'informations

https://chromereleases.googleblog.com/2021/04/stable-channel-update-for-desktop_26.html

Prise de contrôle du système et manipulation de données via 5 vulnérabilités au sein de Microsoft Edge

- Proviennent de Chromium

https://www.cert.ssi.gouv.fr/avis/CERTFR-2021-AVI-311/

Firefox et Firefox ESR, 22 vulnérabilités (mfsa2021-15/mfsa2021-16/mfsa2021-18/ mfsa2021-20)

- Prise de contrôle du système

https://www.mozilla.org/en-US/security/advisories/mfsa2021-15/
https://www.mozilla.org/en-US/security/advisories/mfsa2021-16
https://www.mozilla.org/en-US/security/advisories/mfsa2021-18/
https://www.mozilla.org/en-US/security/advisories/mfsa2021-20

Failles / Bulletins / Advisories
Navigateurs (principales failles)

(exploit) Prise de contrôle du système et divulgation d'informations via une vulnérabilité au sein de Google Chrome (Chromium / CVE-2021-21224)

- Exécution de code arbitraire dans le navigateur

  https://gist.github.com/wdormann/bbf95c5ccebb826a1e21124cfb320106

  https://github.com/avboy1337/1195777-chrome0day

(exploit) Google Chrome, Exec

- Heureusement la sandbox protège.

  https://github.com/rapid7/metasploit-framework/commit/14e22bee37eeff0566cdc32491de0ac9b729aea9

Failles / Bulletins / Advisories
Systèmes

Prise de contrôle du système et manipulation de données via 2 vulnérabilités au sein de Gitlab

- Images mal parsées = RCE
- Update de REXML

https://about.gitlab.com/releases/2021/04/14/security-release-gitlab-13-10-3-released/

Prise de contrôle du système et élévation de privilèges via 14 vulnérabilités au sein de multiples produits SAP (2021-Apr)

- Commerce, NetWeaver…
- Manque de check et injection de code

https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=573801649

Failles / Bulletins / Advisories
Systèmes

Prise de contrôle d'un système et élévation de privilèges via 56 vulnérabilités au sein d'iOS et d'iPadOS (HT212317/HT212336/HT212341)

- RCE Kernel

https://support.apple.com/fr-fr/HT212317
https://support.apple.com/fr-fr/HT212336
https://support.apple.com/fr-fr/HT212341

Prise de contrôle du système et élévation de privilèges via 42 vulnérabilités au sein d'Android (2021-05-01/2021-05-05)

- Dont 3 RCE
- Et moult EoP

https://source.android.com/security/bulletin/2021-05-01

Failles / Bulletins / Advisories
Systèmes

Prise de contrôle du système et élévation de privilèges via 67 vulnérabilités au sein de macOS X (HT212325, HT212326, HT212327, HT212335)

- WebKit

  https://support.apple.com/fr-fr/HT212327
  https://support.apple.com/fr-fr/HT212326
  https://support.apple.com/fr-fr/HT212325
  https://support.apple.com/fr-fr/HT212335

Vulnérabilité dans Python “ipaddress” / CVE-2021-29921

- Mauvaise interprétation d’une IP décimale débutant par 0 considéré comme octal
- Problématique identifiée en … 2019
- Permettrait de faire des SSRF (requête web), RFI et LFI (inclusion de fichiers)

  https://sick.codes/sick-2021-014

Failles / Bulletins / Advisories
Systèmes

NAME:WRECK

- Vulns sur le DNS
- 100 millions de devices potentiellement vulnérables

https://www.bleepingcomputer.com/news/security/name-wreck-dns-vulnerabilities-affect-over-100-million-devices/

tsuNAME

- Attaque DDoS réfléchies
- RFC1536 (Section 2)

https://tsuname.io

Failles / Bulletins / Advisories
Réseau (principales failles)

Cisco

47 bulletins, dont **2 critiques**

- Prise de contrôle du système via 5 vulnérabilités au sein de Cisco SD-WAN
  - CVE-2021-1468
  - CVE-2021-1505
  - CVE-2021-1506
  - CVE-2021-1508
  - CVE-2021-1275
- Prise de contrôle du système via 2 vulnérabilités au sein de Cisco HyperFlex HX
  - CVE-2021-1497
  - CVE-2021-1498

- Produits vulnérables
  - Cisco Access Point Software
  - Cisco Advanced Malware Protection for Endpoints Windows Connector, ClamAV for Windows, and Immunet
  - Cisco Aironet Access Points
  - Cisco IOS and IOS XE Software
  - Cisco IOS XE ROM Monitor Software for Cisco Industrial Switches OS
  - Cisco IOS XE SD-WAN Software
  - Cisco IOS XE SD-WAN Software vDaemon
  - Cisco IOS XE Software
  - Cisco IOS XE Wireless Controller Software for the Catalyst 9000 Family CAPWAP
  - Cisco IOS XR Software
  - Cisco IOx Application Environment Path Traversal Vulnerability
  - Cisco IOx Application Framework
  - Cisco IOx for IOS XE Software
  - Cisco Jabber Desktop and Mobile Client
  - Cisco RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers
  - Cisco SD-WAN vManage
  - Cisco Small Business RV Series Routers
  - Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers Management Interface
  - Cisco Small Business RV132W and RV134W Routers Management Interface
  - Cisco Umbrella Link
  - Cisco Unified Communications Manager

Failles / Bulletins / Advisories
Réseau (principales failles)

Contournement de sécurité et manipulation de données via une vulnérabilité au sein de FortiWAN (FG-IR-21-048)

- Suppression arbitraire de fichier via une requête POST
- Permet le reset du mdp admin

https://www.fortiguard.com/psirt/FG-IR-21-048

Déni de service via 10 vulnérabilités au sein de Stormshield Network Security (STORM-2021-010)

- Erreurs OpenLDAP

https://advisories.stormshield.eu/2021-010/

Failles / Bulletins / Advisories
Réseau (principales failles)

Prise de contrôle du système et manipulation de données via une vulnérabilité au sein de F5

- Contournement du KDC qui permet de s'authentifier directement sur l'interface

https://threatpost.com/f5-big-ip-security-bypass/165735/

Prise de contrôle du système et manipulation de données via 3 0-Day sur SonicWall (SNWLID-2021-0007 / SNWLID-2021-0008 / SNWLID-2021-0010)

- 3 vulns :
  - CVE-2021-20021: création d'un compte d'administration à distance et sans authentification
  - CVE-2021-20022: Possibilité pour un utilisateur authentifié de téléverser un fichier sur la solution
  - CVE-2021-20023: Possibilité pour un utilisateur authentifié de lire n'importe quel fichier
- Exploitées dans la nature
  - Découvertes par encore par FireEye

https://www.sonicwall.com/support/product-notification/security-notice-sonicwall-email-security-zero-day-vulnerabilities/210416112932360/#

https://www.fireeye.com/blog/threat-research/2021/04/zero-day-exploits-in-sonicwall-email-security-lead-to-compromise.html

Failles / Bulletins / Advisories
Réseau (principales failles)

Prise de contrôle du système via 4 vulnérabilités au sein de Pulse Secure (SA44784)

- Welcome back to 2019
- CVE-2021-22893 : exécuter du code à distance sans authentification (CVSS=10 😱)
- Exploitées dans la nature par APT 5 (UNC 2360)
- Découvertes le 20 mars 2021
  - Exploitées depuis l'été 2020
  - Correctif publié en mai 2021 😱

https://twitter.com/mynameisv_/status/1384617771074424836

https://kb.pulsesecure.net/articles/Pulse_Secure_Article/SA44784/

https://www.fireeye.com/blog/threat-research/2021/04/suspected-apt-actors-leverage-bypass-techniques-pulse-secure-zero-day.html

Failles / Bulletins / Advisories
Autre (principales failles)

Prise de contrôle du système et élévation de privilèges via 21 vulnérabilités au sein d'Exim

- PoCs disponibles

  https://www.qualys.com/2021/05/04/21nails/21nails.txt

Spectre strikes back

- Micro-opération oubliée

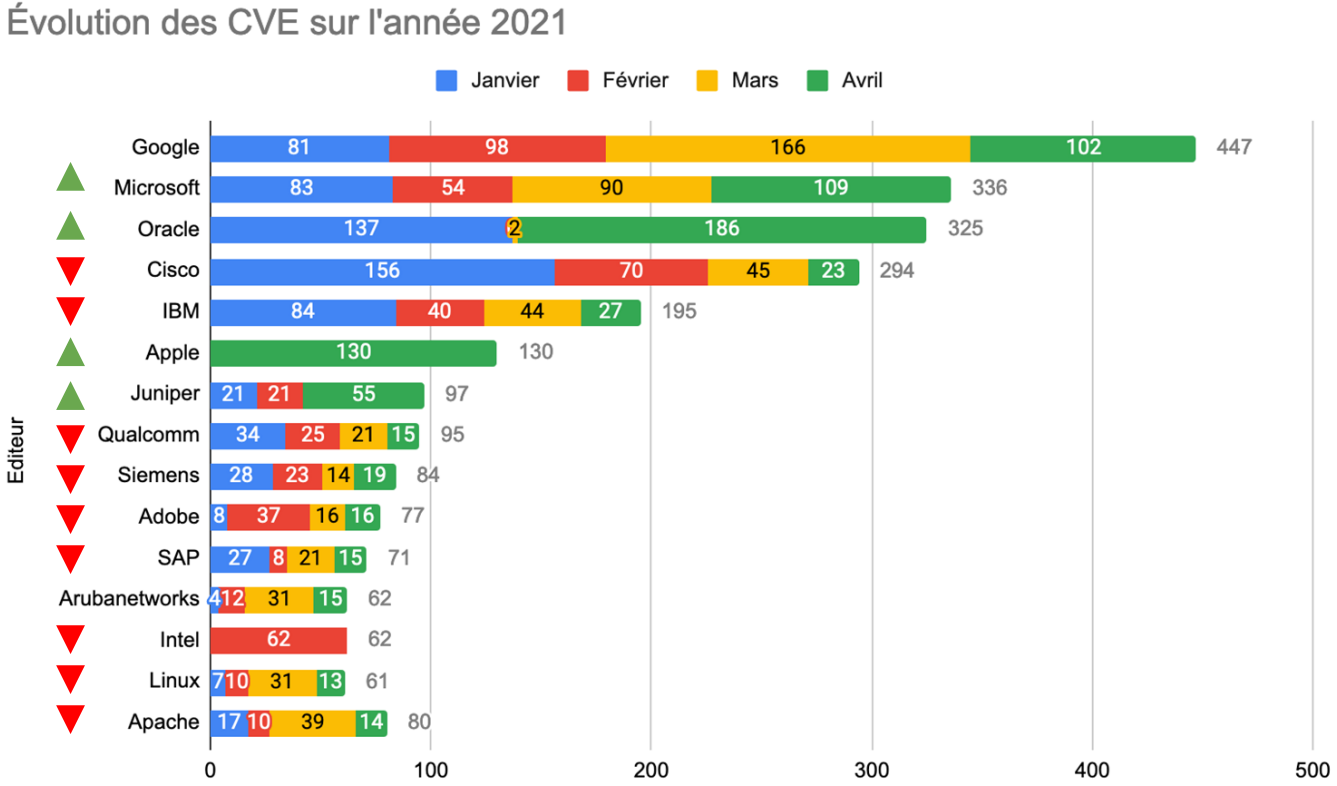
  http://www.cs.virginia.edu/~av6ds/papers/isca2021a.pdf

Vulnérabilité dans exiftool

- RCE en ouvrant une image 

  https://twitter.com/rootxharsh/status/1386343355605417986

Stats du mois



Piratages, Malwares, spam, fraudes et DDoS

Piratages, Malwares, spam, fraudes et DDoS
Piratages

Accellion, solution de transfert de fichiers sécurisés

- Les attaquants utilisent des CVE
- Accellion détecte et corrige…
- Les attaquant utilisent de nouvelles CVE
- Accellion détecte et corrige…
- La sécurité agile…?

https://www.accellion.com/sites/default/files/trust-center/accellion-fta-attack-mandiant-report-full.pdf

Piratages, Malwares, spam, fraudes et DDoS
Piratages

Piratage de gestionnaire de mots de passe Passwordstate (de ClickStudios)

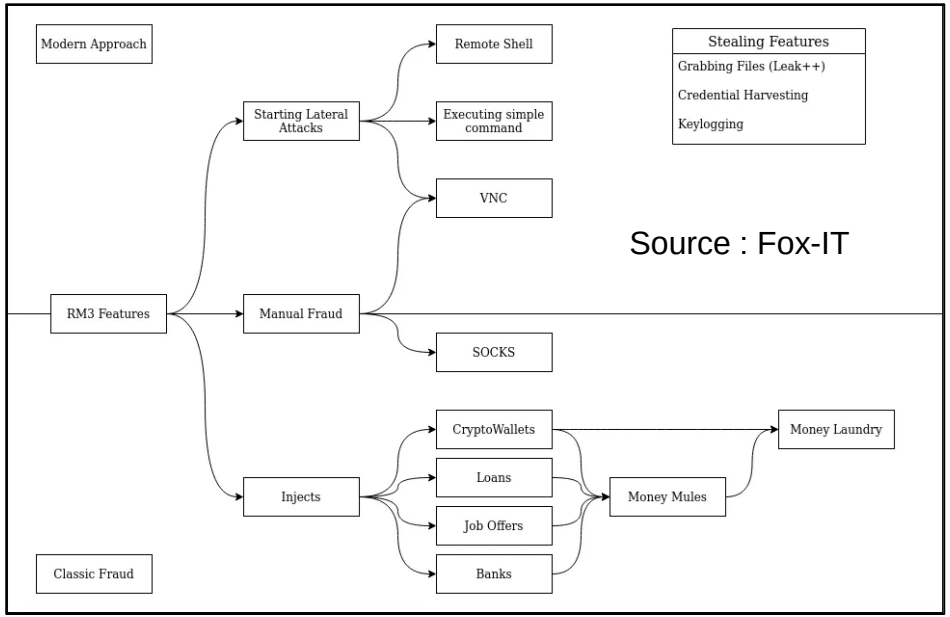
- Attaque de la chaîne d'approvisionnement
- Pour fournir une mise à jour vérolée aux clients

https://www.csis.dk/newsroom-blog-overview/2021/moserpass-supply-chain/

Piratages, Malwares, spam, fraudes et DDoS
Malware

Fox-IT publie un write-up sur RM3

- Lié à Gozi
  https://blog.fox-it.com/2021/05/04/rm3-curiosities-of-the-wildest-banking-malware/



Piratages, Malwares, spam, fraudes et DDoS
Ransomwares

Ryuk : Propagation par un badware

- Torrent -> Badware -> RAT/Keylogger -> RDP -> Ransomware

  https://threatpost.com/ryuk-ransomware-attack-student/165918/

Babuk compromet la Police de Washington D.C.

- Menace de leak des informations sur leurs informateurs

  https://www.theverge.com/2021/4/27/22405339/washington-dc-police-hack-data-department-ransomeware-babuk

Clinique du Grésivaudan

- Visiblement pas d'information exfiltrée

  https://actu.fr/auvergne-rhone-alpes/la-tronche_38516/pres-de-grenoble-la-clinique-du-gresivaudan-victime-d-une-cyberattaque_41142319.html

Piratages, Malwares, spam, fraudes et DDoS
Ransomwares

Groupe DarkSide : Rançonnage d'un pipeline américain

- Blocage du pipeline "Colonial Pipeline"
- Exfiltration de données >100Go

https://www.lemonde.fr/pixels/article/2021/05/10/comment-un-rancongiciel-a-seme-la-panique-dans-un-grand-reseau-d-oleoducs-aux-etats-unis_6079752_4408996.html

Après les paiements en paysafecard et en bitcoin...les paiements en crédit Discord nitro !

- Ransomware nommé GiveMeNitro
- Vol de jeton d'authentification

https://www.bleepingcomputer.com/news/security/discord-nitro-gift-codes-now-demanded-as-ransomware-payments/

Piratages, Malwares, spam, fraudes et DDoS
Hack 2.0 (Supply Chain)

Compromission de Codecov, analyse de code

- Codecov, « code coverage » ou « couverture de code »
- Utilisé par plus de 9000 projets open source

  https://grep.app/search?current=6&q=https%3A//codecov.io/bash

- Modification du script bash hébergé chez codecov
  - https://codecov.io/bash
  - Pas de trace de modification sur leur git
- Extraction des variables d'environnement du projet
- Hashicorp impacté

  https://discuss.hashicorp.com/t/hcsec-2021-12-codecov-security-event-and-hashicorp-gpg-key-exposure/23

  https://therecord.media/codecov-discloses-2-5-month-long-supply-chain-attack/

Compromission de Brew

- Gestionnaire de paquets Mac OS
- Via les GitHub Actions ;)

Piratages, Malwares, spam, fraudes et DDoS
Hack 2.0

Hacking d'une Tesla via un drone

- Pwn2Own
- Possibilité d'ouvrir la voiture à distance via le composant réseau
- Mais ne peuvent pas prendre le contrôle du volant (ouf.)

https://kunnamon.io/tbone/

Les clients de l'opérateur mobile néerlandais KPN pouvait être écouté par Huawei

- Télémaintenance depuis la Chine
- Écoutes légales accessibles

https://www.nextinpact.com/lebrief/46801/huawei-pouvait-ecouter-clients-principal-operateur-mobile-neerlandais

- Le fond du problème : les opérateurs téléphoniques européens ne gèrent plus leur réseau

https://berthub.eu/articles/posts/5g-elephant-in-the-room/

Piratages, Malwares, spam, fraudes et DDoS
Hack 2.0

Vous aussi gagnez de l’argent facilement en partageant vos identifiants

- Fausse société nommée WorkPlace Unite
  https://www.vice.com/en/article/7kvvbb/argyle-payroll-login-phishing

Contourner le mécanisme GateKeeper de MacOS via un document ? C’est possible !

- Erreur de logique dans le moteur de vérification des binaires
  https://objective-see.com/blog/blog_0x64.html

Piratages, Malwares, spam, fraudes et DDoS
Fuites de données

Facebook, numéro 1 des fuites de données

https://securite.developpez.com/actu/314309/Facebook-en-tete-de-liste-du-palmares-des-pertes-de-donnees-d-apres-une-analyse-de-la-societe-Intact-Software/

Piratages, Malwares, spam, fraudes et DDoS
Publication

Nouvelle politique pour Project Zero

- Nouveau délai de disclosure

  https://googleprojectzero.blogspot.com/2021/04/policy-and-disclosure-2021-edition.html

Le modèle 0-Trust vu par l'ANSSI

- Le NIST avait déjà publié un standard

  https://csrc.nist.gov/publications/detail/sp/800-207/final

Rapport d'activité de la cybercriminalité 2020

- Refonte de cybermalveillance.gouv.fr
- Forte composante sur l'ingénierie sociale

  https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/rapport-activite-2020

Piratages, Malwares, spam, fraudes et DDoS
Publication

Analyse de la 1-day Defender (CVE-2021-1647) par les équipes de Project Zero

- Heap overflow
- Recommandations pour corriger cette classe de vulnérabilités

https://googleprojectzero.github.io/0days-in-the-wild//0day-RCAs/2021/CVE-2021-1647.html

Rapport sur l'impact des ransomwares par Kaspersky

- Globalement le nombre de détection est en baisse
- Observent un changement : Les campagnes sont plus ciblées

  https://securelist.com/ransomware-by-the-numbers-reassessing-the-threats-global-impact/101965/

Piratages, Malwares, spam, fraudes et DDoS
Pirater les pirates

Hackback du GRU

- Mot de passe des ressources précédentes : moskva, moskva2
  - Mot de passe ce coup-ci : moskva4
- Question de récupération de compte évidentes (protonmail)
  - Et répondues avec de véritables informations
- Permettant de récupérer des comptes Telegram

  https://twitter.com/christogrozev/status/1384885575073902592

Piratages, Malwares, spam, fraudes et DDoS
Techniques & outils

Playbook de réponse à incident Office 365 / Azure

- Phishing
- Password spray
- App consent grant

https://docs.microsoft.com/en-us/security/compass/incident-response-playbooks

DFIR / OSINT
Techniques & outils

Extracteur de configuration de stealer

- Requêtable via une API (sans authentification !)
- Gère notamment azorult,caliber,citadel,hancitor,icedid,zloader

  https://mwcfg.info

Parlez vous le CTI ?

- Lexique des termes courants

  https://github.com/BushidoUK/CTI-Lexicon/blob/main/Lexicon.md

RSSI/Risk Management
Techniques & outils

CSET v10.2

- Cyber Security Evaluation Tool
- Attention encore quelques soucis...

https://github.com/cisagov/cset

Disponibilité

Nouveau plan “hyper-disponibilité”. chez OVH

- Nouvelles mesures

  https://twitter.com/olesovhcom/status/1389483264230965248?s=19

- Faut-il quitter OVH ?
  - Réponse courte : bien sûr que non !

  https://blog.cozy.io/fr/faut-il-quitter-ovh/

Vie privée
FLoC

Levée de boucliers

- DuckDuckGo

  https://spreadprivacy.com/block-floc-with-duckduckgo/

- WordPress

  https://make.wordpress.org/core/2021/04/18/proposal-treat-floc-as-a-security-concern/

- EFF

  https://www.eff.org/fr/deeplinks/2021/03/googles-floc-terrible-idea

Business et Politique

Business
Monde

Rapid7 acquiert Velocidex

- Velociraptor : Outil d'investigation

https://www.rapid7.com/about/press-releases/rapid7-acquires-digital-forensics-and-incident-response-open-source-project-velociraptor/

Le capital-investissement Thoma Bravo veut acquérir Proofpoint

- Pour $12,3 milliards

https://www.usine-digitale.fr/editorial/le-specialiste-de-la-cybersecurite-proofpoint-rachete-par-thoma-bravo-pour-12-3-milliards-de-dollars.N1086854

LinkByNet en négociation exclusive avec Accenture

- Accenture pourrait absorber LinkByNet

CrowdSec lève 5m€

https://tech.eu/brief/paris-based-crowdsec-raises-5-million-to-firewall-the-world/

Droit / Politique
Monde

Condamnation du cerveau technique du groupe FIN7

- 10 ans de prison

  https://www.cyberscoop.com/fedir-hladyr-fin7-sentencing-prison/

Vulnérabilité d'Exchange

- Pour patcher, exposez votre Exchange sur un VPN sortant avec une IP américaine 💯

  https://www.lemondeinformatique.fr/actualites/lire-le-fbi-autorise-a-nettoyer-a-distance-des-serveurs-exchange-compromis-82599.html

Vulnérabilités Pulse

- La CISA ordonne aux agences fédérales de mettre à jour rapidement

  https://www.bleepingcomputer.com/news/security/cisa-orders-federal-orgs-to-mitigate-pulse-secure-vpn-bug-by-friday/

Mais bientôt, la CISA pourrait aller directement voir les hébergeurs

- Nouveaux droits pour le DHS de faire des injonctions

  https://www.cyberscoop.com/dhs-cyber-alert-subpoena-us/

Droit / Politique
Monde

Procès Apple vs Epic

- Publication de nombreux mails et documents
- 128 millions d'utilisateurs ont téléchargé des applications vérolées
  - Par XCodeGhost

https://twitter.com/patrickwardle/status/1390720904729137158

Conférences

Conférences

Passée

- ...

A venir

- ~~Le Hack -~~ annulé
- Hack-it-n – en distanciel, le 27 mai 2021, à Bodeaux
- SSTIC 2021 - en distanciel, du 2 au 4 juin 2021
- Pass The Salt – en distanciel, du 5 au 7 juillet 2021, à Lille
- BarbHack – en présentiel, le 28 août 2021, à Hyères
- FIC 2021… c'est compliqué :
  - ~~Du 19 au 21 janvier 2021~~
  - ~~Décalé, du 6 au 8 avril 2021~~
  - ~~Décalé, du 8 au 10 juin 2021~~
  - Décalé, en présentiel, du 7 au 9 Septembre 2021 avec CORI&IN le 7 sept.

Divers / Trolls velus

Divers / Trolls velus

Décès de Dan Kaminski

- DNS ne sera plus comme avant

Divers / Trolls velus

Damian Gryski @dgryski · May 8
Just heard about a customer service exploit where the person called up multiple times and corrected a single character "misspelling" until the entire account was in his name.

Mike MacCana @mikemaccana · 23h
"Yeah you have my name misspelt as "Mike" but it's actually "Sike", ess aye kay ee."

Mike MacCana @mikemaccana · 15h
"Hi yeah it's Stike here. I spoke to Carol earlier, she was fixing my name. I think she actually set it it to 'Sike' but forgot the t."

a person @cryptoyeezy · 9h
"Hi, yes, my account name is misspelled. It's Stive, not Stike."

@mikko @mikko · 6h
"Hi, it's me again, Stivo"

Zé Vinícius @mircaze · 4h
"Hello, it's Stevo calling, uh..."

a person @cryptoyeezy · 23m
"Hahaha, I know right? How hard is it to spell Steve? There must have been a bad connection at the time. Well, thanks for fixing it, James, really appreciate the help."

Zé Vinícius @mircaze · 18m
"Hi James, it's Steven again. How you doing?"

Robert Lowery
@DaTechGuy

"Hi, is Carol or James available?" "Off shift? Ok"

"They were trying to help me fix spelling issues on my account. Yeah, it is Stevenson and it is actually my last name."

https://twitter.com/dgryski/status/1125922800877883393

Divers / Trolls velus

Microsoft migre au SHA2

- Dès Mai 2021 😱

  Tout va bien se passer ‘v’

  https://techcommunity.microsoft.com/t5/windows-it-pro-blog/microsoft-to-use-sha-2-exclusively-starting-may-9-2021/ba-p/2261924

Flacon parmi les 3 finalistes du NIST Post-Quantum Cryptography

- Pour la partie “Digital Signature Algorithms”

  https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions

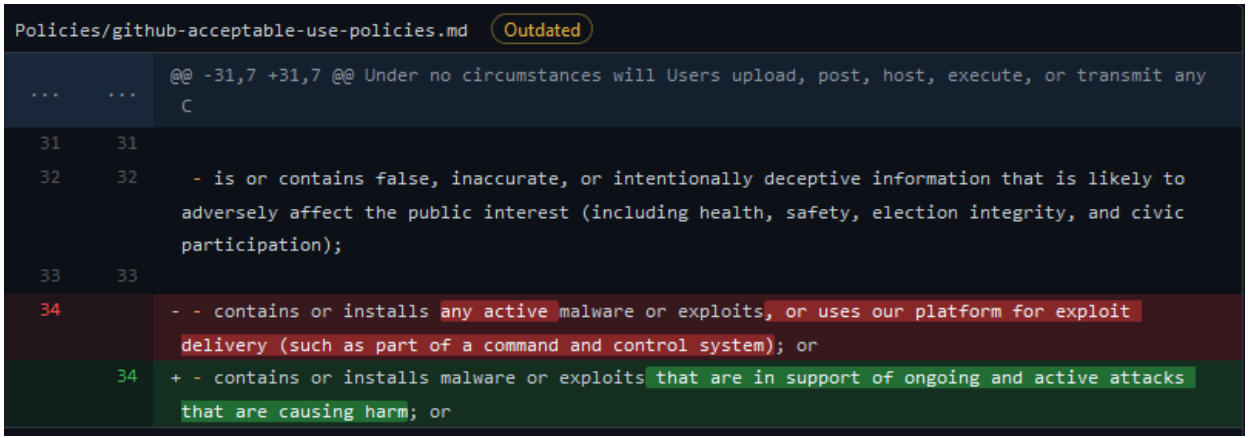
- Thales y participe avec un de ses salariés dans l’équipe
- Vu par France Info : <<Thales met au point une protection contre la cybercriminalité quantique du futur>>

  https://www.francetvinfo.fr/replay-radio/nouveau-monde/nouveau-monde-thales-met-au-point-une-protection-contre-la-cybercriminalite-quantique-du-futur_4383879.html

Divers / Trolls velus

Mise à jour de la politique de Github (appartenant à Microsoft)

- Risque de l'interdiction d'y stocker des exploits, outils offensifs...
  https://github.blog/2021-04-29-call-for-feedback-policies-exploits-malware/
- Mise à jour :



Divers / Trolls velus

Apple peut accéder à la quasi totalité des données sur iCloud

- Etat de l'art de la sécurité des smartphones
  https://securephones.io/main.html
- La KeyChain serait aussi accessible
  https://www.youtube.com/watch?v=afA3QNw4QUY

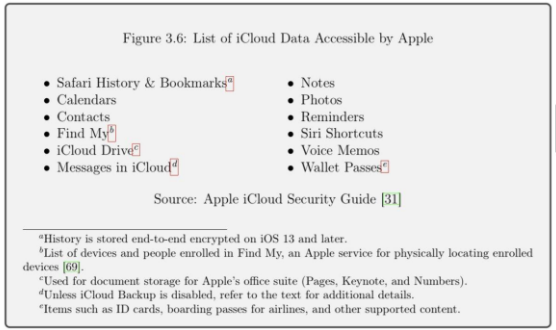


Figure 3.6: List of iCloud Data Accessible by Apple

- Safari History & Bookmarks[a]
- Calendars
- Contacts
- Find My[b]
- iCloud Drive[c]
- Messages in iCloud[d]
- Notes
- Photos
- Reminders
- Siri Shortcuts
- Voice Memos
- Wallet Passes[e]

Source: Apple iCloud Security Guide [31]

[a]History is stored end-to-end encrypted on iOS 13 and later.
[b]List of devices and people enrolled in Find My, an Apple service for physically locating enrolled devices [69].
[c]Used for document storage for Apple's office suite (Pages, Keynote, and Numbers).
[d]Unless iCloud Backup is disabled, refer to the text for additional details.
[e]Items such as ID cards, boarding passes for airlines, and other supported content.

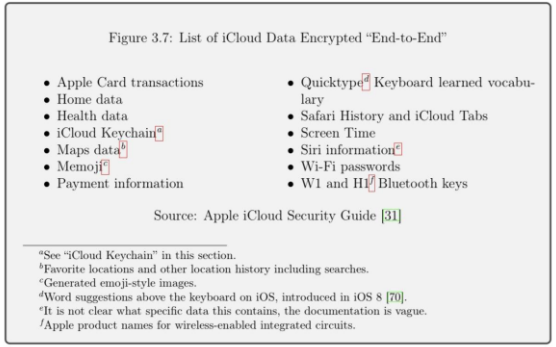


Figure 3.7: List of iCloud Data Encrypted "End-to-End"

- Apple Card transactions
- Home data
- Health data
- iCloud Keychain[a]
- Maps data[b]
- Memoji[c]
- Payment information
- Quicktype[d] Keyboard learned vocabulary
- Safari History and iCloud Tabs
- Screen Time
- Siri information[e]
- Wi-Fi passwords
- W1 and H1[f] Bluetooth keys

Source: Apple iCloud Security Guide [31]

[a]See "iCloud Keychain" in this section.
[b]Favorite locations and other location history including searches.
[c]Generated emoji-style images.
[d]Word suggestions above the keyboard on iOS, introduced in iOS 8 [70].
[e]It is not clear what specific data this contains, the documentation is vague.
[f]Apple product names for wireless-enabled integrated circuits.

RSA est cassé ? <<This destroys the RSA cryptosystem.>>

- Papier très sérieux de Claus Peter Schnorr
  https://eprint.iacr.org/2021/232
- Selon Schneier, non
  - https://www.schneier.com/blog/archives/2021/03/no-rsa-is-not-broken.html
- Amélioration probable des techniques actuelles
- Mais RSA ne devrait plus être utilisé depuis des années…
  - Clef trop longues, risques de factorisation...

Divers / Trolls velus

Panne chez Fortnite

- A cause de l'expiration d'un certificat

  https://www.epicgames.com/site/en-US/expiration-date-4-6-2021

Trump est un agent russe

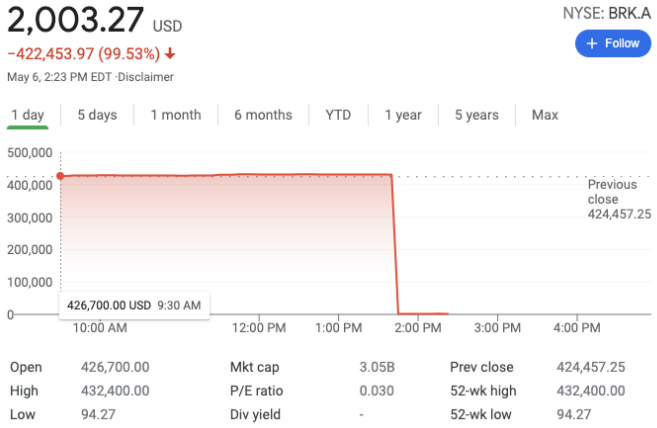
- Un rapport de la CIA, du FBI… classifié du temps de Trump, déclassifié
- Le rapport considère Trump comme un agent russe

  https://slate.com/news-and-politics/2021/03/trump-russian-asset-election-intelligence-community-report.amp

Quand le prix de l'action dépasse MAX_INT32

- 2^32 = 4 294 967 296 (en non signé)
- ici en milliardièmes, soit $429 496,7296

  https://twitter.com/MathisHammel/status/1390645858178379784



Divers / Trolls velus

Cyber assurance, ça bouge !

- Entreprises avec assurance Cyber en France :
  - 2018 : 50%
  - 2019 : 60%
- L'Anssi et le parquet de Paris reprochent aux assureurs d'encourager les rançongiciels payant
- Axa ne paiera plus en France

https://hotforsecurity.bitdefender.com/blog/insurer-axa-says-it-will-no-longer-cover-ransomware-payments-in-france-25793.html

Des groupes de rançongiciel tentent spéculation à la baisse sur le cours de bourse

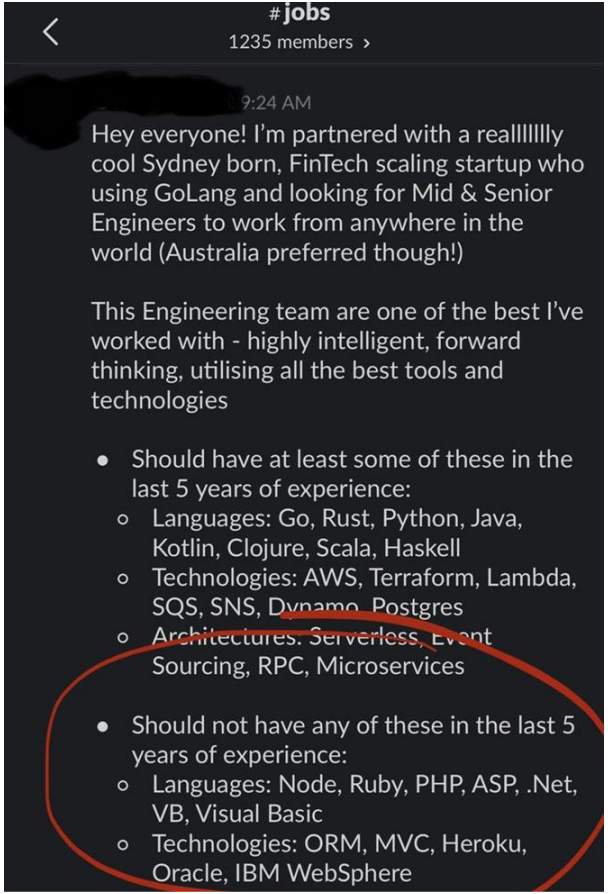
- Mais…
  - Les transactions sont tracées et identifiées
  - Les gendarmes boursiers locaux risquent de ne pas laisser faire

https://therecord.media/ransomware-gang-wants-to-short-the-stock-price-of-their-victims/

Divers / Trolls velus

Le recrutement en 2021…

https://twitter.com/wabzqem/status/1378894021397909506



Divers / Trolls velus

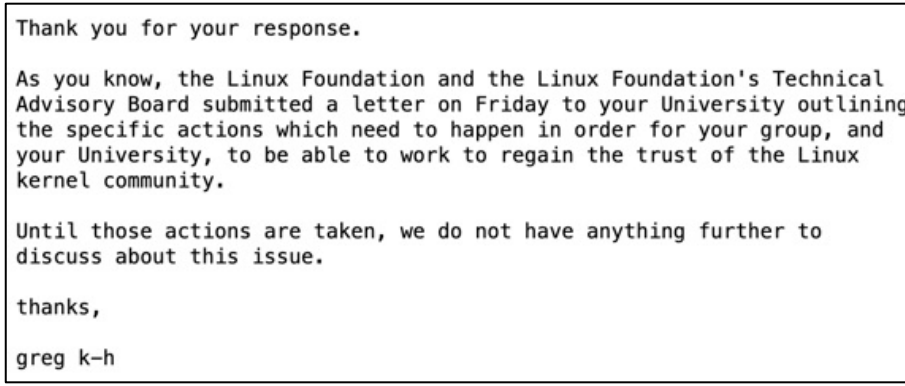
L’université du Minnesota, bannie du LKML

- Que se passerait-t-il si on essayait d’introduire subtilement des failles de sécurité dans des projets open-source via des commits hypocrites ?
- Réponse : Un bannissement.
  - Le souci c’est que ces essais ont continués après la publication du premier whitepaper
  - Des excuses ont été formulées mais...

https://raw.githubusercontent.com/QiushiWu/qiushiwu.github.io/main/papers/OpenSourceInsecurity.pdf

On the Feasibility of Stealthily Introducing Vulnerabilities in Open-Source Software via Hypocrite Commits

Qiushi Wu and Kangjie Lu
University of Minnesota
{wu000273, kjlu}@umn.edu



```
Thank you for your response.

As you know, the Linux Foundation and the Linux Foundation's Technical
Advisory Board submitted a letter on Friday to your University outlining
the specific actions which need to happen in order for your group, and
your University, to be able to work to regain the trust of the Linux
kernel community.

Until those actions are taken, we do not have anything further to
discuss about this issue.

thanks,

greg k-h
```

Divers / Trolls velus

Signal tacle Cellebrite

- Moxie Marlinspike, CEO de Signal, a réalisé quelques recherches sur UFED
- Des Centaines de vulnérabilités
  - Des logiciels et librairies non à jour depuis 1000 ans
  - Librairies pour différents formats de fichiers : images, vidéos, données de Whatsapp, sms, contacts…

https://signal.org/blog/cellebrite-vulnerabilities/

Prochaines réunions

Prochaine réunion

- 8 juin 2021… toujours en visio

After Work

- Pas avant ~~Q3~~ Q4 2021 ?

Questions ?

Des questions ?

- C’est le moment !

Des idées d’illustrations ?

Des infos essentielles oubliées ?