

[Tous](#) [Actualités](#) [Images](#) [Produits](#) [Vidéos](#) [Web](#) [Livres](#) [Plus](#)[Outils](#)

## À la une :

### Attaque contre le système d'information de l'AFP

**01Net**

Une mystérieuse cyberattaque frappe l'Agence France-Presse

il y a 14 minutes

**Siècle Digital**

Cyberattaque majeure contre l'AFP : une menace inédite pour le journalisme...



il y a 2 heures

**Mac4Ever**

Cyberattaque : L'Agence France-Presse a été ciblée

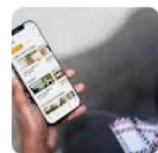


il y a 3 heures

### Meilleurtaux alerte ses clients sur une cyberattaque

**BFMTV**

Revenus, situation familiale... Meilleurtaux victime d'une fuite de...



il y a 21 heures

**01Net**

Fuite de données en France : une nouvelle victime confirme une cyberattaque



il y a 1 jour

### Également dans les actualités

**DNA**

Eschau. La mairie victime d'une cyberattaque depuis plusieurs jours



il y a 22 heures

**Media24.fr**

3AS Racing : la renaissance après une cyberattaque historique pour ce...



il y a 2 jours

## Cyberattaque :

[Plus d'images](#)

Une cyberattaque est un acte offensif envers un dispositif informatique à travers un réseau cyberspace. Une cyberattaque peut émaner de personnes isolées ou d'un groupe de pirates informatiques, éventuellement étatique.

[Wikipédia](#)[Commentaires](#)

# La CNIL alerte sur une explosion des cyberattaques

Le gendarme des données personnelles a enregistré 5.037 notifications de violation de données en 2021, soit une hausse de 79 % sur un an. Elles concernent notamment près de 2.200 attaques par rançongiciel.

France 24  
23/08/22

FRANCE 24

#ELIZABETH II #GUERRE EN UKRAINE FRANCE AFRIQUE REPORTAGES EMISSIONS STOP L'INFO

RANÇONGICIEL

EN DIRECT

Budget

Cyberattaque d'un hôpital : un mode opératoire classique mais des exigences démesurées

Publié le : 23/08/2022 - 17:17



Le Centre hospitalier sud francilien, d'une capacité d'un millier de lits, fonctionne au ralenti depuis une cyberattaque dans la nuit du samedi 20 au dimanche 21 août. © Joël Saget, AFP

Texte par : Sébastien SEIBT [Suivre](#) 6 mn

Le Centre hospitalier sud francilien demeure sous l'emprise d'un virus de type rançongiciel trois jours après avoir subi une cyberattaque dans la nuit de samedi à dimanche. Les assaillants ont suivi le modus operandi classique pour ce genre d'opération à un détail près : la rançon de 10 millions de dollars exigée paraît absurde pour un établissement public de santé.

Accueil > Business > Industrie > L'industrie de la mode doit aussi se protéger des vagues de cybercriminalité



## L'industrie de la mode doit aussi se protéger des vagues de cybercriminalité

Elina S. 16 août 2022 Industrie, Sécurité Ecrire un commentaire

Chaque étape vers la numérisation de bout en bout du secteur de la mode suggère une plus grande exposition à la cybercriminalité. Avec la croissance des boutiques en ligne, l'essor des usines intelligentes et la mise en place des assistants virtuels au niveau du support client, l'industrie de la mode prend-elle les mesures nécessaires pour se protéger des vagues d'attaques ?

lebigdata.fr  
10/08/22



En direct



Le Journal



Newsletters

...

CONNEXION



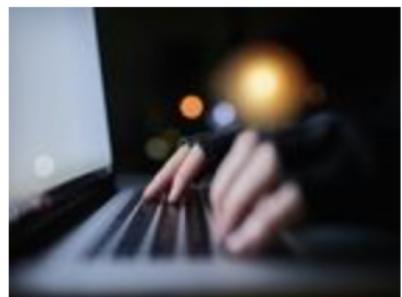
Idées Économie Élections Entreprises Finance - Marchés Bourse Monde Tech-Médias Start-up Politique Régions Patrimoine Le Mag \

## Les cyberattaques contre les banques ont triplé pendant le confinement

Le secteur bancaire s'est retrouvé davantage exposé aux cyberattaques pendant le confinement.

Le recours accru au télétravail a ouvert des brèches que les cybercriminels exploitent pour soutirer de l'argent ou des données.

### La Corée du Nord a tenté de pirater 11 membres du Conseil de sécurité de l'ONU



Sécurité - Un nouveau rapport du Conseil de sécurité de l'ONU révèle que des membres du Conseil de sécurité ont été pris pour cible à plusieurs reprises au cours de l'année écoulée.

Jeudi 01 Octobre 2020 par Catalin Cimpanu

[Réagissez !](#)

### Chantage numérique : ça ne touche pas que les riches



Sécurité - Le mois d'octobre est à nouveau l'occasion de sensibiliser le public sur les risques liés à la cybercriminalité. Avec cette année, un sujet qui coule de source : celui du chantage numérique, qui ne touche pas que les grands comptes.

Jeudi 01 Octobre 2020 par [Louis Adam](#)

[Réagissez !](#)

L



### Microsoft : certaines attaques prennent moins de 45min



Sécurité - Microsoft passe en revue les récentes tendances en matière de logiciels malveillants dans son nouveau "Digital Defense Report".

Mercredi 30 Septembre 2020 par Catalin Cimpanu

[Réagissez !](#)

---

## L'industrie maritime en alerte après le piratage de l'armateur français CMA-CGM



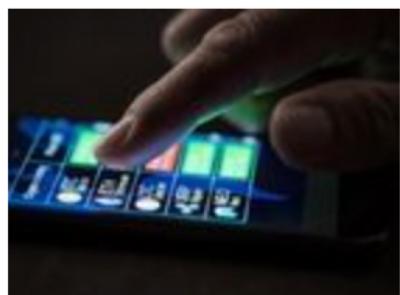
*Technologie* - Après le piratage du géant français du transport maritime CMA-CGM, touché par un ransomware, ce sont désormais les quatre géants du secteur qui ont été victime de campagne de cyberattaque depuis 2017.

Mardi 29 Septembre 2020 par Catalin Cimpanu

Réagissez !

---

## Cryptomonnaie : la plateforme KuCoin victime d'un piratage de grande ampleur



*Technologie* - La plateforme d'échange de cryptomonnaie KuCoin a été touchée par une vaste campagne de piratage. Les pirates ont réussi à subtiliser pour 150 millions de dollars de fonds.

Lundi 28 Septembre 2020 par Catalin Cimpanu

1 commentaire



INFORMATIQUE

## Les services de la ville de Besançon victimes d'une cyberattaque

Anne Vignot, la maire, a appelé ses administrés et administrées à la vigilance



CYBERSECURITE

## Android : Une faille dans le Bluetooth expose les utilisateurs

Bien que Google ait été mis au courant, aucune mise à jour correctrice n'est encore disponible

⌚ 14/08/20 | 0 | 112



CYBERATTAQUE

## Le Vatican ciblé par des hackers

Les pirates informatiques à l'origine de l'attaque seraient proches du gouvernement chinois

⌚ 30/07/20 | 3 | 61



ESPIONNAGE

## 4G : Une faille réseau expose les appels téléphoniques aux hackers

Une vulnérabilité au sein du réseau 4G LTE permet aux hackers d'espionner les appels téléphoniques

⌚ 17/08/20 | 2 | 13



RANÇONGICIEL

## Garmin a été piratée, des avions n'ont pas pu décoller aux Etats-Unis

L'attaque a empêché les opérations de mise à jour des bases de données et de planification des vols, pour lesquels les outils numériques de l'entreprise sont utilisés

⌚ 28/07/20 | 5 | 126



PIRATAGE

## Des milliers de comptes de services gouvernementaux piratés au Canada

Les attaques ont visé le service CléGC, utilisé par une trentaine de ministères fédéraux, et des comptes de l'Agence du revenu du Canada

⌚ 16/08/20 | 17 | 329

## Voiture connectée...

Charlie Miller et Chris Valasek (BlackHat2015) :  
prise de contrôle à distance d'une Jeep



TOUTE L'ACTUALITÉ / SÉCURITÉ  
**Chrysler rappelle 1,4 million de voitures exposées à un piratage à distance**

, publié le 27 Juillet 2015

- Cause : de nombreux services non sécurisés en écoute sur internet
- Combien de systèmes (pacemakers, voitures, avions, usines., réseaux de distribution..) reposent de manière critique sur du logiciel pour fonctionner ?

# MS17-010 : la menace des rançongiciels [O. Levillain]

En mai et juin 2017



- Deux attaques très médiatisées par des rançongiciels
  - exploitation d'une vulnérabilité critique dans Windows
  - ... sur un service qui ne devrait pas être exposé
  - ... pour lequel un correctif est disponible depuis mars
- Pourquoi la sécurité semble-t-elle un échec?

## Objectif du cours

- Acquérir les éléments pour une confiance mesurée dans le numérique;
- Donner un éclairage sur les technologies de sécurité : actuelles et perspectives futures

Quelle confiance dans le numérique?

# Cours – WMMMBESEC

## Sécurité Informatique et confidentialité

Jean-Louis ROCH

- Un aperçu général et des approfondissements techniques sur les éléments principaux qui définissent la sécurité d'un système informatique, avec un accent particulier sur les certificats et la dimension intégrité et confidentialité des données.
- Documents de référence: documents de l'ANSSI (tenus à jour)
  - Transparents : **Contenu pédagogique CyberEdu** : <https://www.cyberedu.fr/>
  - « **Bonnes pratiques** » : <https://cyber.gouv.fr/bonnes-pratiques-protegez-vous>
  - « **Renforcer la sécurité de son système d'information en 42 mesures** » (2017) <https://cyber.gouv.fr/actualites/le-nouveau-guide-dhygiene-informatique-renforcer-la-securite-de-son-systeme-dinformation>
  - **Référentiel Général de Sécurité (RGS)** <https://cyber.gouv.fr/le-referentiel-general-de-securite-rgs>

# De nombreux supports disponibles (documents, logiciels, etc)

Exemple: <https://developer.ibm.com/patterns>

The screenshot shows the IBM Developer website at <https://developer.ibm.com/patterns>. The page title is "Code Patterns". On the left, there's a sidebar with "Build smart." and "Build secure." text, and a "Technologies" section with checkboxes for Blockchain (checked), Analytics, Artificial intelligence, Containers, Conversation, Data management, Data science, and Data stores. A "Show more" link is also present. The main content area shows "Showing 1 - 12 of 68 results" and three code pattern cards. The first card, "Build a secure microservices-based banking application" (August 25, 2020), shows a hand holding a smartphone displaying a banking app interface. The second card, "Perform analytics on blockchain transactions" (April 2, 2020), shows a hand holding a smartphone displaying a car's front end. The third card, "Use access control in your blockchain smart contracts to streamline supply chain operations" (March 26, 2020), shows a red lanyard with a white badge. A "Sort: Date Newest to Old" dropdown is visible in the top right. A "Site feedback" link is on the far right.

Build smart.  
Build secure.

Code Patterns

Technologies

Blockchain

Analytics

Artificial intelligence

Containers

Conversation

Data management

Data science

Data stores

Show more

Industries

Showing 1 - 12 of 68 results

Sort: Date Newest to Old

Code Pattern

Build a secure microservices-based banking application

August 25, 2020 →

Code Pattern

Perform analytics on blockchain transactions

April 2, 2020 →

Code Pattern

Use access control in your blockchain smart contracts to streamline supply chain operations

March 26, 2020 →

Site feedback



ANSSI

Agence nationale de la sécurité des  
systèmes d'information

Déclaration vulnérabilité

En cas d'incident

Alertes

Presse

Recrutement

## Par thèmes

TITRE	THEME	DATE	
	<b>RECOMMANDATIONS POUR LA SÉCURISATION DE LA MISE EN OEUVRE DU PROTOCOLE OPENID CONNECT</b> 08/09/2020 authentification fournisseur d'identité fournisseur de service OAuth2.0 OpenID Connect SSO		<a href="#">PDF 794.45 Ko</a> 
	<b>ATTAQUES PAR RANÇONGICIELS, TOUS CONCERNÉS - COMMENT LES ANTICIPER ET RÉAGIR EN CAS D'INCIDENT ?</b> 04/09/2020 chiffrement collectivité crise cybercriminalité entreprise Gestion des risques rançongiciel ransomware sensibilisation		<a href="#">PDF 963.63 Ko</a> 
	<b>RECOMMANDATIONS POUR LES ARCHITECTURES DES SYSTÈMES D'INFORMATION SENSIBLES OU DIFFUSION RESTREINTE</b> 28/08/2020 administration architecture chiffrement défense en profondeur diffusion restreinte DR II 901 information sensible interconnexion Internet nomadisme passerelle réglementation supports amovibles		<a href="#">PDF 3.05 Mo</a> 
	<b>RÈGLES DE PROGRAMMATION POUR LE DÉVELOPPEMENT SÉCURISÉ DE LOGICIELS EN LANGAGE C</b> 21/07/2020 bonne pratique C89/C90 C99 développement sécurisé langage C recommandation règle		<a href="#">PDF 974.81 Ko</a> 
	<b>PROFIL DE FONCTIONNALITÉS ET DE SÉCURITÉ - SAS ET STATION BLANCHE (RÉSEAUX NON CLASSIFIÉS)</b> 01/07/2020 SaaS Station blanche supports amovibles transfert de fichier USB		<a href="#">PDF 1.24 Mo</a> 

> *Tous les thèmes*> *Applications Web*> *Cryptographie*> *Dispositifs de vidéoprotection*> *Externalisation*> *Liaisons sans fil et mobilité*> *Méthodologie*> *Poste de travail et serveurs*> *Réseaux*> *Systèmes industriels*

## **Exemple: Guide sur la sécurité des mots de passe (ANSSI 25/05/2012)**

- La robustesse d'un mot de passe dépend en général d'abord de sa complexité, mais également de divers autres paramètres, expliqués en détail dans le document « Recommandations de sécurité relatives aux mots de passe ».
- Si vous souhaitez une règle simple : choisissez des mots de passe d'au moins 12 caractères de types différents (majuscules, minuscules, chiffres, caractères spéciaux).  
Deux méthodes pour choisir vos mots de passe :
  - La méthode phonétique : « J'ai acheté huit cd pour cent euros cet après-midi » deviendra ght8CD%E7am ;
  - La méthode des premières lettres : la citation « un tien vaut mieux que deux tu l'auras » donnera 1tvmQ2tl'A.
- Ou utilisez un gestionnaire de mots de passe...

# Plan du cours

<https://chamilo.grenoble-inp.fr/courses/ENSIMAGWMMBESEC/>

Calcul note = 50% TP + 50% Devoirs à la maison

## 1. Cours 3h Introduction. Confiance numérique: bonnes-pratiques [Jean-Louis Roch]

- Principes de base sur la sécurité des systèmes . Analyse DICP.
- Clefs, Chiffrements symétrique et asymétrique, signature, hachage
- Travail à la maison DM 0 (non noté) : ssh et certificats
- Confiance dans son système d'information: bonnes pratiques.
- Présentation du DM 1 (à rendre pour le 24/11/2022)

## 2. Cours + TP [Mathias Ramparison] - Virtualisation et blockchain - Analyse de faille

- Présentation du DM 2 - Venez avec votre poste de travail !

## 3. Cours 9h Confiance numérique [Jean-Louis Roch]

- Architectures de confiance (PKI centralisées et distribuées) et certificats
- Cours Blockchain et TP Blockchain (Mathias Ramparison)
- Protocoles multiparties
- Perspectives avec les certifications interactives
- Intégrité des protocoles industriels
- bonnes-pratiques - Retours sur le DM 1

# Vulnérabilités : <https://www.cve.org>

https://cve.mitre.org

## Common Vulnerabilities and Exposures

The Standard for Information Security Vulnerability Names

Follow CVE [Twitter](#) [LinkedIn](#)

Home | CVE IDs | About CVE | CVE in Use | Community & Partners | Blog | News | Site Search

TOTAL CVE IDs: 91302

Become a CNA  
Click for process, documentation & more

Request a CVE ID  
Click for CNAs, MITRE request form, guidelines, & more

Update info in a CVE ID  
Click for MITRE request form, guidelines & more

CVE List downloads  
Available in xml, CVRF, txt, & comma-separated

CVE content data feed  
Available via CVEnew Twitter Feed

### CNA Participation Growing Worldwide

CVE Numbering Authorities (CNAs)  
Totals CNAs: 77 | Total Countries: 14

CNAs include vendors and projects, vulnerability researchers, national and industry CERTs, and bug bounty programs.

CNAs are how the CVE List is built. Every CVE ID added to the list is assigned by a CNA.

### Latest CVE News

- ASUSTOR Added as CVE Numbering Authority (CNA)
- CVE Replaces "CVE Compatibility Program" with CVE Compatibility Guidance Document
- Minutes from CVE Board Teleconference Meeting on September 20 Now Available
- Forcepoint Added as CVE Numbering Authority (CNA)

More >

### CVE Blog

#### Become a CVE Numbering Authority

CVE Numbering Authorities, or "CNAs," are how the CVE List is built. Every CVE ID added to the list is assigned by a CNA.

The majority of CNAs are currently software vendors that assign CVE IDs to issues in their own products, but many vulnerability researchers and third-party coordinators also participate by assigning CVE IDs to issues in third-party products per their specified scopes of coverage.

As of today, there are 77 total CNAs participating in the CVE program from around the world with 14 countries now represented.

Please consider joining us as a CNA ...

### New CVE IDs

Tweets by @CVEnew

**CVE** @CVEnew  
CVE-2017-15185 plugins/ogg.c in Libmp3splt 0.9.2 calls the libvorbis vorbis\_block\_clear function with ... [bit.ly/2y4ZQV](#)  
2h

**CVE** @CVEnew  
CVE-2017-14973 IDentocard Two-Reader Controller Configuration Manager 1.18.8 (396) is vulnerable to Stored ... [bit.ly/2wHZ2xL](#)  
2h

**CVE** @CVEnew  
CVE-2017-14972 InFocus Mondopad 2.2.08 is vulnerable to authentication bypass when accessing uploaded files by ... [bit.ly/2fX9pXu](#)  
2h

**CVE** @CVEnew

# CVE tweets

Twitter, Inc. (US) | https://twitter.com/CVEnew/ | Rechercher | Vous avez déjà un compte ? Se connecter | Accueil | À propos | Recherchez sur Twitter | Suivre

The screenshot shows the Twitter profile for @CVEnew. The header features the CVE logo and the text "Common Vulnerabilities and Exposures". The profile summary indicates 9,352 tweets, 2 subscriptions, and 3,873 followers. The tweets section displays five recent posts from the CVE account, each detailing a specific software vulnerability and linking to a detailed report. The sidebar includes sections for "Nouveau sur Twitter?" (with a "S'inscrire" button) and "Tendances : Monde" (listing trending topics like #Estamos Unidos Mexicanos, #FelizLunes, etc.).

**Tweets**

**Tweets & réponses**

**CVE** @CVEnew · 2 h CVE-2017-15185 plugins/ogg.c in Libmp3split 0.9.2 calls the libvorbis vorbis\_block\_clear function with ... bit.ly/2y42ZQV

**CVE** @CVEnew · 2 h CVE-2017-14973 IDentocard Two-Reader Controller Configuration Manager 1.18.8 (396) is vulnerable to Stored ... bit.ly/2wHZ2xL

**CVE** @CVEnew · 2 h CVE-2017-14972 InFocus Mondopad 2.2.08 is vulnerable to authentication bypass when accessing uploaded files by ... bit.ly/2fx9pXu

**CVE** @CVEnew · 2 h CVE-2017-14971 Infocus Mondopad 2.2.08 is vulnerable to a Hashed Credential Disclosure vulnerability. The ... bit.ly/2y3yOti

**CVE** @CVEnew · 6 oct. CVE-2015-2673 The ec\_ajax\_update\_option and ec\_ajax\_clear\_all\_taxrates functions in ... bit.ly/2fRhXIE

**Nouveau sur Twitter ?**

Inscrivez-vous maintenant pour obtenir votre fil d'actualités personnalisé !

**S'inscrire**

**Tendances : Monde**

- #Estamos Unidos Mexicanos 🇲🇽 160 k Tweets
- #FelizLunes 7 884 Tweets
- #HIAC 240 k Tweets
- #EyAmerika 7 401 Tweets
- #MasterChefMx 🍜 41,9 k Tweets
- صلاح الخير 17,4 k Tweets
- Delhi-NCR 3 235 Tweets
- Los Ángeles Azules 6 032 Tweets

CVE-ID	
<b>CVE-2017-15185</b>	<a href="#">Learn more at National Vulnerability Database (NVD)</a> • Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings
Description	plugins/ogg.c in Libmp3splt 0.9.2 calls the libvorbis vorbis_block_clear function with uninitialized data upon detection of invalid input, which allows remote attackers to cause a denial of service (application crash) via a crafted file.
References	<p><b>Note:</b> <a href="#">References</a> are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.</p> <ul style="list-style-type: none"><li>• EXPLOIT-DB:42399</li><li>• URL:<a href="https://www.exploit-db.com/exploits/42399/">https://www.exploit-db.com/exploits/42399/</a></li><li>• MISC:<a href="http://seclists.org/fulldisclosure/2017/Jul/82">http://seclists.org/fulldisclosure/2017/Jul/82</a></li><li>• MISC:<a href="https://anonscm.debian.org/cgit/users/ron/mp3splt.git/commit/?id=18f018cd774cb931116ce06a520dc0c5f9443932">https://anonscm.debian.org/cgit/users/ron/mp3splt.git/commit/?id=18f018cd774cb931116ce06a520dc0c5f9443932</a></li><li>• MISC:<a href="https://lists.debian.org/debian-its/2017/09/msg00115.html">https://lists.debian.org/debian-its/2017/09/msg00115.html</a></li></ul>
Assigning CNA	MITRE Corporation
Date Entry Created	<b>20171008</b> <small>Disclaimer: The entry creation date may reflect when the CVE-ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.</small>
Phase (Legacy)	Assigned (20171008)

# Ce qu'on a vu

- 1. Les enjeux de la sécurité des S.I.**
- 2. Les besoins de sécurité : critères DICP**
- 3. Notions de vulnérabilité, menace, attaque**
- 4. Panorama de quelques menaces**
- 5. Le droit des T.I.C. et l'organisation de la sécurité en France**