Breizh Cyber

Région Bretagne

COMMUNIQUÉ DE PRESSE

Le jeudi 27 juin 2024, à Rennes

A l'initiative de Breizh Cyber et avant les Jeux Olympiques

Les centres régionaux de réponse cyber se mobilisent pour les collectivités

A l'initiative de Breizh Cyber, le centre de réponse aux incidents (CSIRT) de la Région Bretagne, et en partenariat avec l'éditeur en cybersécurité ONYPHE, les CSIRT régionaux français et les centres de ressources cyber (CRC) ultra-marins se sont unis pour mener une campagne de recherche en vulnérabilité au profit des collectivités locales. Cette campagne d'envergure a eu lieu en avril, sur l'ensemble du territoire français. Cette initiative, rendue possible grâce à la politique d'ouverture des données de l'État, vise à renforcer la sécurité informatique des collectivités territoriales à l'approche des Jeux olympiques de Paris 2024.

L'open data au service de la cybersécurité

La campagne de recherche en vulnérabilités a été réalisée grâce à l'**exploitation de bases de données publiques de l'administration**. Ce ne sont pas moins de **25 000 noms de domaines** d'entités publiques parmi les communes, intercommunalités, conseils départementaux, centres de gestion territoriaux et conseils régionaux, qui ont été analysés. Cette démarche innovante a permis aux CSIRT régionaux d'**identifier les failles de sécurité** au sein des systèmes d'information des collectivités locales, et ce de manière massive.

En s'appuyant sur ces données ouvertes, ce sont ainsi **186 entités publiques** qui ont été identifiées comme présentant des équipements **vulnérables à 311 failles critiques,** parmi les 25 000 analysés, soit un taux de **0,73% du total.** Un chiffre **plutôt rassurant** au regard du volume de la cohorte analysée.

Les **failles les plus fréquentes** concernent des logiciels de **messagerie (Microsoft Exchange, Zimbra)** ou de **gestion de parc informatique (GLPI).**

> ***Résultats détaillés en pages suivantes.***

Accompagner les collectivités pour mieux les protéger

Cette campagne illustre la montée en puissance et la force du collectif des CSIRT régionaux et des CRC ultra-marins. En unissant leurs moyens, notamment pour **avertir les entités publiques** concernées et **les accompagner** dans la correction des vulnérabilités identifiées, les centres cyber français se mobilisent pour renforcer la cybersécurité des collectivités locales.

Ainsi, à la date du 26 juin, **25% des vulnérabilités** identifiées en avril avaient été **corrigées** grâce à l'action coordonnée des CSIRT régionaux et des CRC ultra-marins auprès des propriétaires des équipements concernés.

Renforcement de la sécurité à l'approche des JO

À moins de 100 jours des Jeux olympiques de Paris 2024, la **sécurité informatique des collectivités** locales est plus que jamais **une priorité**. Cette campagne contribue ainsi à renforcer la sécurité des systèmes d'information des collectivités locales, afin de **garantir la continuité et la résilience de leurs services** lors de cet événement majeur.


© Adobe Stock

À propos de Breizh Cyber

Lancé en 2023 par la Région, Breizh Cyber est le centre de réponse aux incidents de sécurité informatique, dédié aux entreprises, associations et collectivités locales du territoire breton. Breizh Cyber analyse et répond à la menace ou redirige vers des spécialistes locaux certifiés.

Ses équipes de proximité sont joignables au 0800 200 008 ou via le site breizhcyber.bzh.

SERVICE PRESSE

02 99 27 13 54 | presse@bretagne.bzh

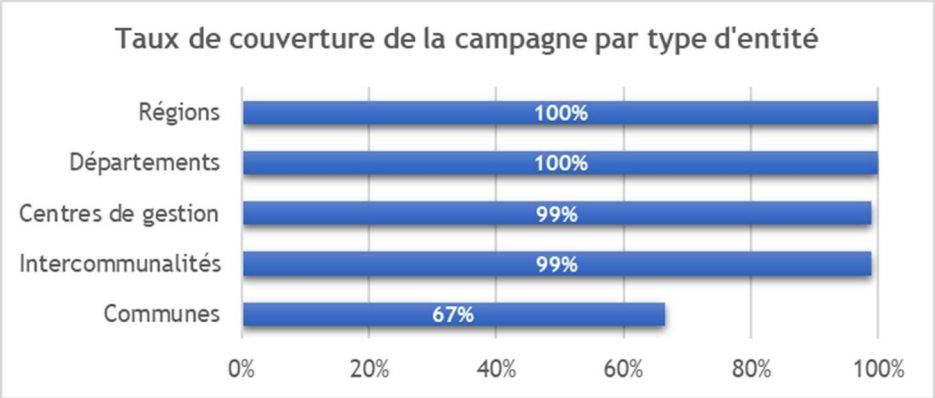
Odile Bruley (06 76 87 49 57) | Sylvain Le Duigou (06 42 32 13 57) | Aymery Bot (07 50 12 41 30) | Sébastien Jédor (06 22 49 94 69)

www.bretagne.bzh/espace-presse @bretagne_presse

Annexe : résultats de la campagne

Nombre d'entités publiques analysées

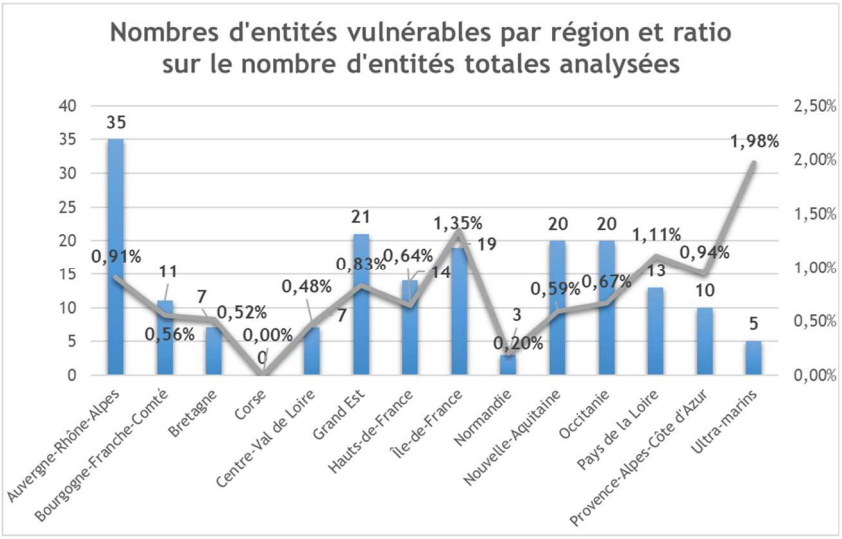
Le nombre d'entités analysées (par unités de noms de domaine) est de 25 334. Cela représente la couverture suivante par types d'entités publiques. La source des données est l'API des services publics et plus particulièrement l'API annuaire des établissements publics de l'administration. Concernant les communes, le taux de couverture est de 67% soit par le fait que le nom de domaine n'est pas renseigné dans l'annuaire des services publics soit par le fait que la commune ne s'est pas dotée d'un site web, ce qui est le cas pour les plus petites communes. La campagne a été réalisée du 2 au 10 avril 2024.



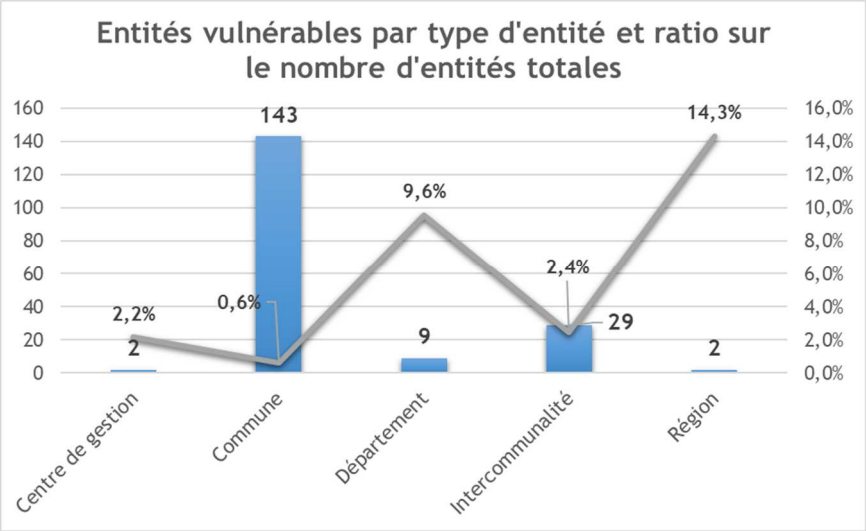
Résultats de la campagne

186 entités sont vulnérables à au moins une faille critique soit 0,73% du total. 311 failles critiques uniques ont été identifiées au total.

La répartition des entités présentant au moins une vulnérabilité par territoire est la suivante. Le résultat fait apparaître une variabilité peu significative entre les territoires.



La répartition des entités présentant au moins une vulnérabilité par type d'entité est la suivante. Le résultat fait apparaître les communes comme les plus représentées en nombre absolu mais le plus faible en ratio.



Le top des vulnérabilités identifiées les plus fréquentes

Sur les vulnérabilités les plus fréquemment identifiées, 10 sur 12 avaient fait l'objet d'un bulletin d'alerte du CERT-FR c'est-à-dire présentant un danger immédiat. L'objectif de la campagne était de se concentrer sur les risques les plus importants.

Top	CVE	Technologie concernée	Score CVSS	Date de publication
1	CVE-2022-41082	Microsoft Exchange « ProxyNotShell »	8.8	30/09/2022
2	CVE-2023-20032	Zimbra	9.8	16/02/2023
3	CVE-2023-42802	GLPI	9.8	26/09/2023
4	CVE-2022-27925	Zimbra	7.2	30/08/2022
5	CVE-2022-37042	Zimbra	9.8	28/10/2022
6	CVE-2021-31207	Microsoft Exchange « ProxyShell »	6.6	12/05/2021
7	CVE-2021-34523	Microsoft Exchange « ProxyShell »	9	15/07/2021
8	CVE-2021-34473	Microsoft Exchange « ProxyShell »	9.1	16/07/2021
9	CVE-2024-21893	Ivanti	8.2	01/02/2024
10	CVE-2023-7028	Gitlab	7.5	12/01/2024
11	CVE-2023-27997	Fortinet	9.8	12/06/2023
12	CVE-2024-21888	Ivanti	8.8	01/02/2024

Outil d'analyse utilisé

ONYPHE est un moteur de recherche dédié à la cyberdéfense, spécialisé dans la découverte et la gestion de la surface d'attaque. Cette solution n'est pas un scanner de vulnérabilités. L'outil ne vérifie pas de manière exhaustive toutes les vulnérabilités mais que les failles les plus critiques reconnues comme activement exploitées par les groupes d'attaquants. Cela représente à date une centaine de vulnérabilités.

Breizh Cyber