Bug de l'an 2038 (Le)

Titre(s) : Bug de l'an 2038 (Le) [[periodique]] / Muriel Valin

Ensemble : Epsiloon 57

Auteur(s) : Valin, Muriel

Editeur, producteur : 01/03/26

Description matérielle : pp.20-27

ISSN : 2800-4736

Note sur la description matérielle : 7

Résumé ou extrait : Le bug de l'an 2038 vient du codage du temps Unix sur 32 bits : le 19 janvier 2038 à 3 h 14 min 7 s UTC, la valeur maximale sera atteinte et, à la seconde suivante, certains systèmes reviendront au 13 décembre 1901 à 20 h 45 min 52 s, provoquant erreurs, arrêts ou blocages. Longtemps cantonné au monde des développeurs, le risque a refait surface avec le contentieux entre la RATP et Alstom. Découvert le 5 octobre 2017 sur une rame MI09 incapable d'accepter une date au-delà de 2037, le défaut a conduit à l'analyse de 261 logiciels embarqués du RER A : 38 étaient vulnérables, ainsi que des équipements de huit lignes de métro et six lignes de tramway, soit environ un tiers du réseau. Après une demande de réparation déposée le 9 juin 2020, le tribunal administratif de Paris a ordonné le 5 décembre 2025 à Alstom de proposer en trois ans une solution pour les matériels concernés.L'enquête montre que l'enjeu dépasse largement les transports : dispositifs médicaux, infrastructures industrielles, banques, distributeurs automatiques, équipements de bâtiments, télécoms, routeurs, imprimantes ou logiciels anciens peuvent être touchés. Beaucoup de ces systèmes, installés dans les années 1990 et 2000, ont une durée de vie de 30 à 40 ans, ne sont pas toujours connectés à distance et ne font l'objet d'aucun inventaire précis. Les spécialistes estiment que le parc potentiellement concerné est 500 à 600 fois plus vaste que celui du bug de l'an 2000, dont la correction avait coûté 150 milliards d'euros en Europe et mobilisé des équipes pendant une dizaine d'années.Les solutions techniques existent, comme la migration vers 64 bits, l'utilisation du 32e bit jusqu'en 2106, le changement de processeur ou l'abandon de l'heure Unix, mais aucune n'est simple ni peu coûteuse. Elles supposent souvent de relire d'anciens codes en Cobol, assembleur ou C, parfois sans documentation ni auteurs encore présents. Une étude japonaise sur 32 921 projets en langage C publiés sur GitHub entre 2012 et 2018 a montré que 7,35 % étaient vulnérables. Des incidents ont déjà eu lieu chez KDDI en 2004, AOL en 2006 ou Proton Calendar en 2022, et des experts alertent aussi sur le risque de cyberattaques exploitant cette faille. Fin 2025, l'Union internationale des télécommunications a validé un document appelant à une coordination mondiale, tandis que la loi européenne sur la cyberrésilience, votée en 2024 et applicable en 2027, pourrait accélérer la mise à jour des systèmes embarqués....

Sujet - Titre uniforme : UNIX

Sujet - Nom commun : Logiciels -- Prévention
Métros, Matériel roulant -- France -- Paris