Guillaume QUÉRÉ
Ingénieur sécurité, 32 ans
prime@errno.fr

Compétences

Langages	**C**, **Python**, **Bash**	Root-Me	10000+ points, Top 20
Systèmes	**Linux**, Windows	GitHub	github.com/gquere
Outils	vim, gcc, GNU Make, git, gdb, IDA	Site	www.errno.fr
Autres	Électronique, **tests d'intrusion**		
Anglais	Bilingue		

Expérience professionnelle

2016 - 2021 (5 ans) — **Enedis (ex-ERDF) –** La Défense
Tests d'intrusion software/hardware des compteurs Linky : électronique, fuzzing protocolaire
Tests d'intrusion du SI Linky : audit de code (C, PHP, Python, Bash, Java), audit système (Linux, Windows), reverse engineering, recherche de vulnérabilités, Active Directory
C, Python, PHP, JTAG, CPL, Linux

2014 - 2016 (2 ans) — **AIRBUS Defence & Space –** Élancourt
Architecture, développement et intégration de la partie système (init & configuration) et DPI (capture, extraction de métadonnées, traitement, analyse) d'une sonde réseau.
Refonte du workflow (git, process de livraison) et formation des équipes.
C, Python, Git, Unit testing, Jenkins, Debian packaging, méthode agile

2013 (1 an) — **SagemCom –** Rueil-Malmaison
Portage du savoir-faire Sagem (routing et vidéo) dans une gateway d'architecture nouvelle.
Intégration de middleware et de drivers d'un parti tiers.
Développement driver GPIO/interrupts, mécanisme de synchronisation entre CPUs.
Buildroot, OpenWRT, SVN, GNU Make, KBuild, C, shell script

2012 (6 mois) — **Zodiac SIT –** Plaisir
Sécurisation d'un système de divertissement avionique : stack USB du kernel Linux, intégration secure boot u-boot, automatisation de gestion de droits SSH, module PAM/OPIE, authentification de flux vidéo, architecture, provisioning de secrets et de données.
Debian squeeze, GPXE, U-Boot, Git, Wiki, C, shell script, VLC

Recherche

Vulnérabilités
CVE-2017-6913 : Stored XSS dans Open-Xchange
10+ CVE Centreon : RCE, auth bypass, XSS, SQLi...
RCE BMC Control-M
RCE, Privesc BMC Patrol
Bypass d'authentification Pulse Secure SSL VPN
10+ vulnérabilités DELL EMC (en cours de correction) : RCE, auth bypass
2 vulnérabiliés Barebox (en cours de correction) : temporal side-channel

Développement
ngp : outil facilitant l'audit de code/conf
Toolkits d'exploitation : Jenkins, injection .NET, Artifactory, mRemoteNG, bloodhound Linux, ...

Communauté
Administrateur du site Root-Me : modération, tests, publication, création de challenges ...
Présentations dans des conférences (BeerRump, SSTIC)
Contributeur régulier du podcast « Le Comptoir Sécu »
Articles techniques sur mon site : www.errno.fr

Formation

2010 - 2012 — **RWTH Aachen,** échange Erasmus
ECE – École Centrale d'Électronique, ingénieur diplômé 2012
Systèmes embarqués, section internationale.

2006 - 2010 — **ESTACA**, Master 1 mécanique

Autres

CTF : finaliste challenge SSTIC 2020, HtB, Root-Me ...
Permis de conduire, tous les points.
Nombreuses références sur demande.