CVE-2017-7344 Fortinet FortiClient Windows privilege escalation at logon

CLÉMENT NOTIN (HTTPS://SECURITE.INTRINSEC.COM/AUTHOR/CLEMENT-NOTIN/) × 22 DÉCEMBRE 2017

Summary

Editor: Fortinet

Product: FortiClient

Title: Fortinet FortiClient Windows privilege escalation at logon

CVE ID: CVE-2017-7344 (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7344)

Intrinsec ID: ISEC-V2017-01

Risk level: high

Exploitable: Locally, or remotely if the logon screen is exposed (e.g. through RDP without NLA required). Requires non-default configuration on the client (« Enable VPN before logon »). Requires an invalid certificate on the VPN endpoint side, or a MITM attacker presenting an invalid certificate (e.g. stolen laptop scenario).

Impact: Privilege escalation: from anonymous to SYSTEM, and Windows lock screen bypass

Description

This vulnerability affects the Fortinet FortiClient program. FortiClient is a client program used to connect to SSL/IPsec VPN endpoints.

A setting, disabled by default, enables FortiClient on the logon screen to allow users to connect to a VPN profile before logon. An attacker, with physical, or remote (e.g. through TSE, VNC...), access to a machine with FortiClient and this feature enabled, can obtain SYSTEM level privileges from the lock screen. No account or prior knowledge is required.

The vulnerability lies in the confirmation dialog shown when the server certificate is not valid (e.g. default auto-signed certificate, or Man-In-The-Middle with SSL/TLS interception situation).

Versions affected

- FortiClient Windows 5.6.0
- FortiClient Windows 5.4.3 and earlier

Solutions

Upgrade to FortiClient Windows 5.4.4 or 5.6.1.

However, we tested the latest version and we discovered some bypasses of the fix under certain circumstances. We have shared our findings with Fortinet who is working on a more complete fix. We do not intend to share more details until this issue is fixed.

Enabling the « Do not warn invalid server certificate » option would prevent this issue but it is strongly discouraged since it allows silent Man-in-the-Middle attacks.

Deploying a valid certificate on the VPN endpoint mitigates the issue in standard situations, however when an attacker is in a MITM situation they will present an invalid certificate to the FortiClient, regardless of the legitimate server certificate. This is not sufficient to resolve the issue.

Credits

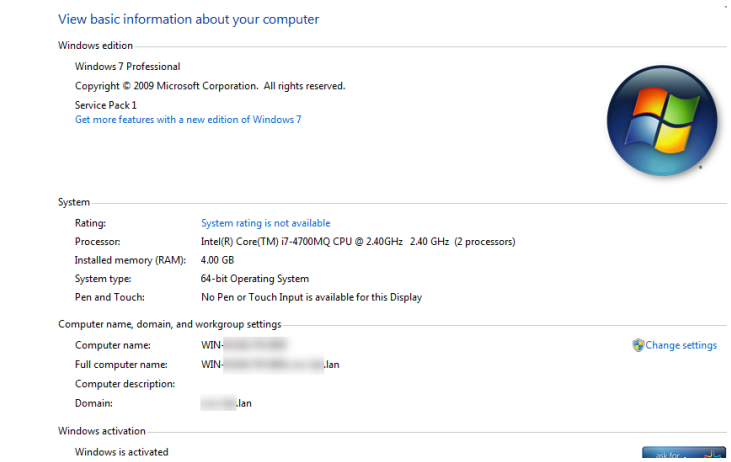
Vulnerability discovered by Clément Notin / @cnotin (https://twitter.com/cnotin).

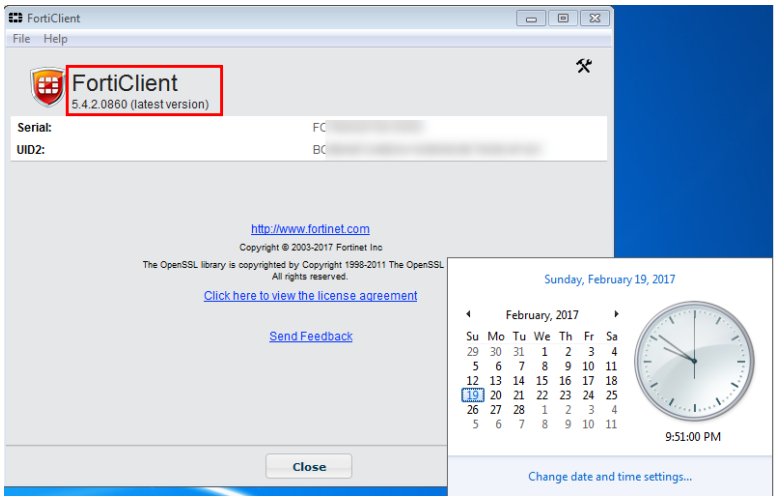
Vulnerability disclosed in coordination with the CERT-Intrinsec.

Exploitation details

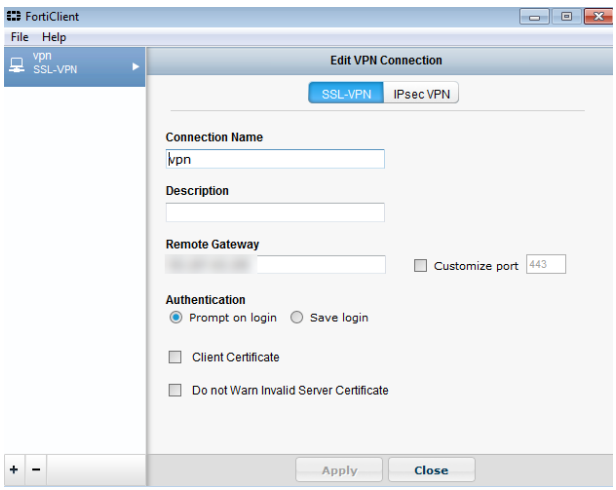
Setup

Windows 7 Professional x64, English. FortiClient, vulnerable version:

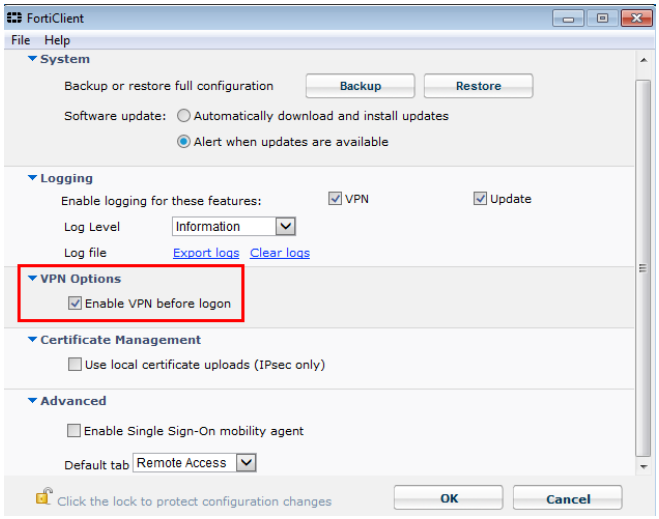




Create VPN connection in FortiClient with a FortiGate endpoint (or try with any domain having an invalid certificate, such as expired.badssl.com):



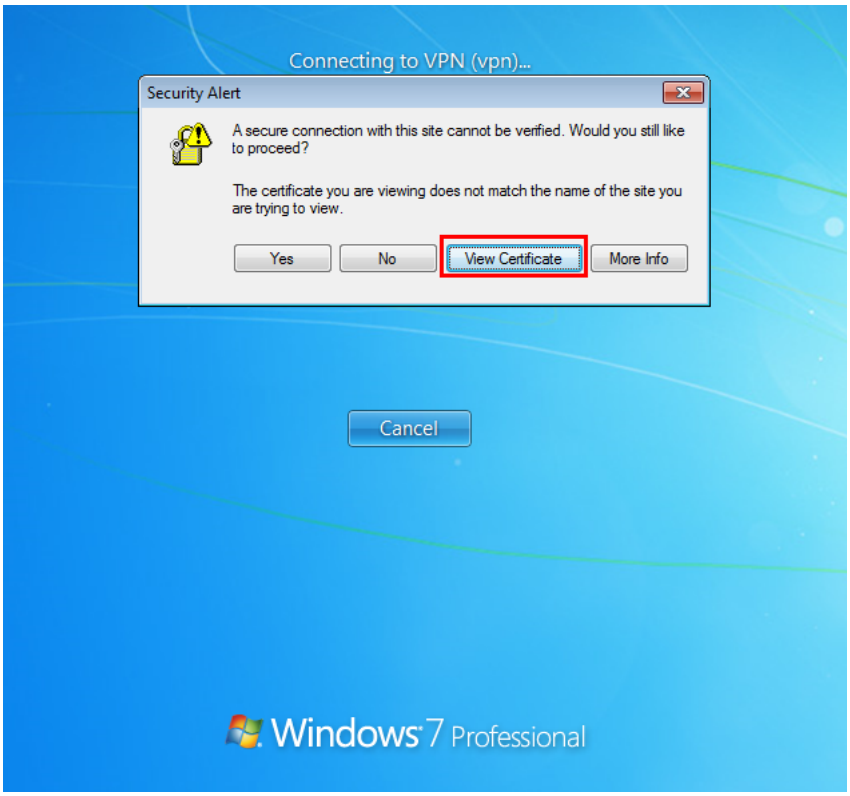
Enable the "VPN before logon" setting in FortiClient:



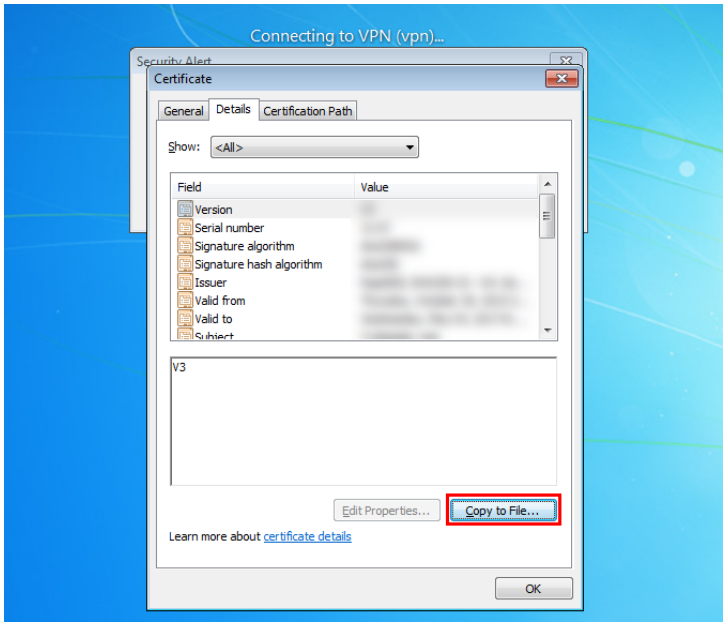
Log off. The computer is now in a vulnerable state.

Exploitation steps

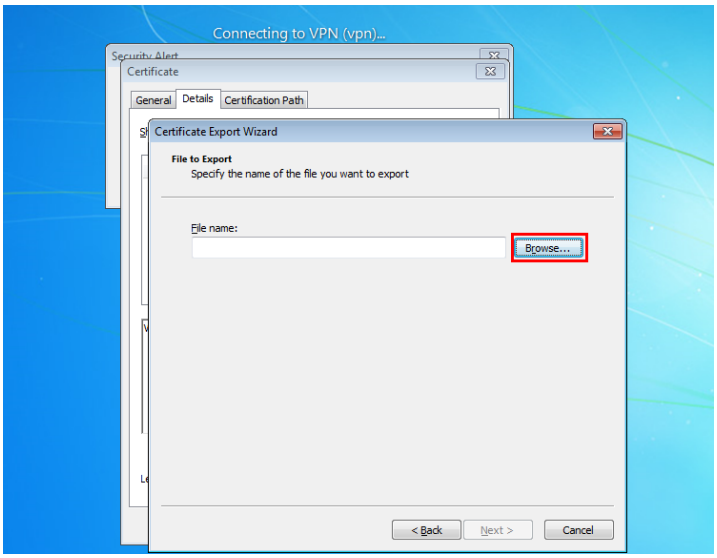
On the logon screen, select the VPN profile and type any password for the user. If the certificate is invalid (default certificate on a legitimate FortiGate, MITM attack, usage of the IP address of the endpoint instead of the hostname…), when connecting the confirmation dialog will appear, then click on “View certificate”:



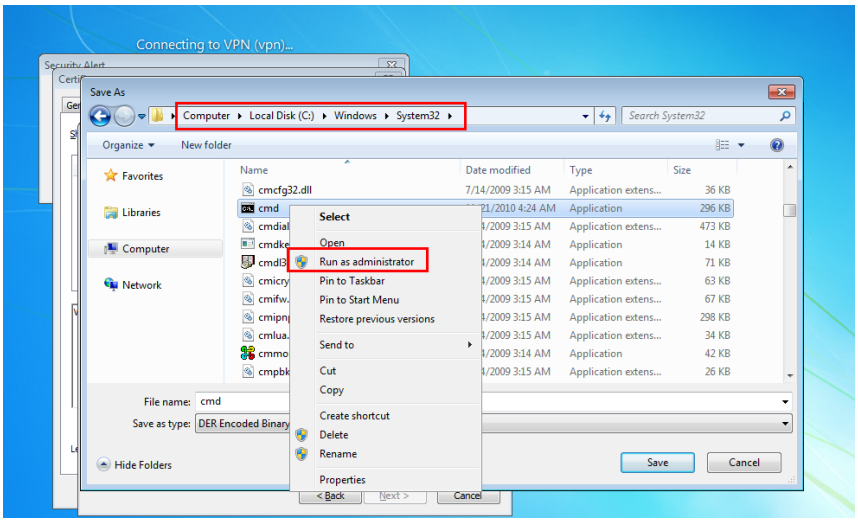
Go to “Details” tab then click on “Copy to file”:



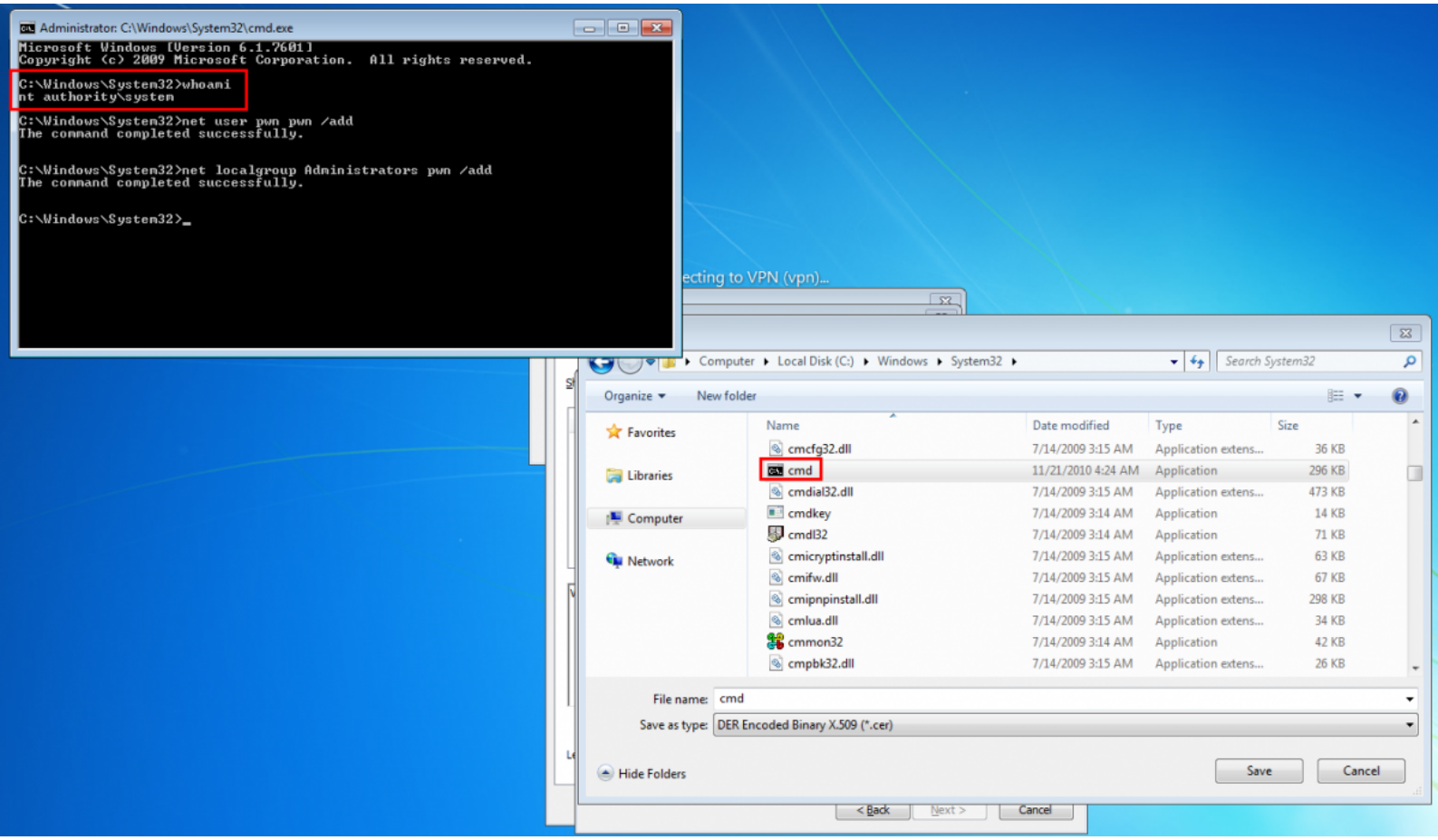
Click next until the screen with “Browse” button:



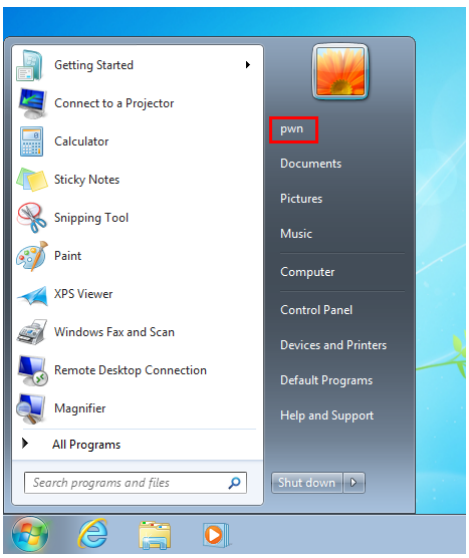
Browse to “C:\Windows\System32”, type a wildcard “*” in filename to show every files. Find cmd.exe, right click then click “Open”:



You get a shell with SYSTEM privileges:



The attacker can create a local administrator user account and use it to login:



External references

Fortinet PSIRT Advisory: FG-IR-17-070 (https://fortiguard.com/psirt/FG-IR-17-070)

CERT-FR: CERTFR-2017-AVI-471 (https://www.cert.ssi.gouv.fr/avis/CERTFR-2017-AVI-471/)

SecurityFocus: BID 102176 (http://www.securityfocus.com/bid/102176)

Mitre: CVE-2017-7344 (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7344)

History

- 2017-02-27: Vulnerability discovery, advisory sent to Fortinet that acknowledges the reception.
- 2017-03-15: Intrinsec asks for status update
- 2017-05-04: Fortinet confirms the vulnerability, assigns CVE-2017-7344 and plans the fix for the future 5.6 version.
- 2017-06-08: ETA for fixed versions set in June
- 2017-07-05: Intrinsec asks for status update
- 2017-07-11: Intrinsec discovers that FortiClient 5.6.0.1075, that was supposed to include the fix, is still vulnerable
- 2017-08-25: Fortinet clarifies the purpose of the fix and confirms that it is incomplete. New ETA is set to end of September for FortiClient 5.6.1.
- 2017-12-07: Intrinsec asks for status update
- 2017-12-11: Fortinet is finalizing the advisory and plans to publish it during the week
- 2017-12-13: Fortinet publishes the advisory
- 2017-12-13: Intrinsec advises against some proposed mitigations
- 2017-12-13: Fortinet updates the advisory
- 2017-12-18: Intrinsec finds bypasses of the published fix and shares the details with Fortinet
- 2017-12-21: Fortinet confirms the bypasses
- 2017-12-22: Intrinsec publishes its advisory with detailed explanations, with Fortinet's approval

— Clément Notin

7344%0D%0A%0D%0AIntrinsec%20ID%3A%C2%A0ISEC-V2017-01%0D%0A%0D%0ARisk%20level%3A%20high%0D%0A%0D%0AExploitable%3A%20Locally%2C%20or%20remotely%20if%20the%20logon%20scre)

ARTICLE PRÉCÉDENT (HTTPS://SECURITE.INTRINSEC.COM/2017/12/13/BOTCONF-2017-JOUR-3/)

BOTCONF 2017 - TROISIÈME JOURNÉE (HTTPS://SECURITE.INTRINSEC.COM/2017/12/13/BOTCONF-2017-JOUR-3/)

PAS DE NOUVEAUX ARTICLES

CLÉMENT NOTIN (HTTPS://SECURITE.INTRINSEC.COM/AUTHOR/CLEMENT-NOTIN/)

(//www.twitter.com/cnotin)

ARTICLES SIMILAIRES

UNE RÉPONSE

27 décembre 2017 (https://securite.intrinsec.com/2017/12/22/cve-2017-7344-fortinet-forticlient-windows-privilege-escalation-at-logon/#comment-9966)

Jesus Hack (http://s/n)

Répondre (https://securite.intrinsec.com/2017/12/22/cve-2017-7344-fortinet-forticlient-windows-privilege-escalation-at-logon/?replytocom=9966#respond)

hi
i have a doubt
This vulnerability was aprove with SO Windows 8, 8.1 and 10 , or only with windows 7

ECRIRE UN COMMENTAIRE

Votre adresse e-mail ne sera pas publiée.

COMMENTAIRE

NOM*

E-MAIL*

SITE WEB

ECRIRE UN COMMENTAIRE

NEWSLETTER

Recevez notre veille sécurité et les actualités d'Intrinsec (retours d'expériences, communications, ...)

Votre adresse mail

S'inscrire

ARTICLES RÉCENTS

- CVE-2017-7344 Fortinet FortiClient Windows privilege escalation at logon (https://securite.intrinsec.com/2017/12/22/cve-2017-7344-fortinet-forticlient-windows-privilege-escalation-at-logon/)
- Botconf 2017 – troisième journée (https://securite.intrinsec.com/2017/12/13/botconf-2017-jour-3/)
- Botconf 2017 – deuxième journée (https://securite.intrinsec.com/2017/12/12/botconf-2017-jour-2/)
- Botconf 2017 – première journée (https://securite.intrinsec.com/2017/12/11/botconf-2017-jour-1/)
- Hack.lu 2017 (https://securite.intrinsec.com/2017/10/20/hack-lu-2017/)

MOTS CLEFS

ACTIVE DIRECTORY (HTTPS://SECURITE.INTRINSEC.COM/TAG/ACTIVE-DIRECTORY/) ALCATEL (HTTPS://SECURITE.INTRINSEC.COM/TAG/ALCATEL/) ANDROID (HTTPS://SECURITE.INTRINSEC.COM/TAG/ANDROID/) APACHE (HTTPS://SECURITE.INTRINSEC.COM/TAG/APACHE/) BREIZHCTF (HTTPS://SECURITE.INTRINSEC.COM/TAG/BREIZHCTF/) CERT (HTTPS://SECURITE.INTRINSEC.COM/TAG/CERT/) CLUSIR (HTTPS://SECURITE.INTRINSEC.COM/TAG/CLUSIR/) CONFÉRENCE (HTTPS://SECURITE.INTRINSEC.COM/TAG/CONFERENCE/) CTF (HTTPS://SECURITE.INTRINSEC.COM/TAG/CTF/) DOS (HTTPS://SECURITE.INTRINSEC.COM/TAG/DOS/) ESGI (HTTPS://SECURITE.INTRINSEC.COM/TAG/ESGI/) GESTION DE VULNÉRABILITÉS (HTTPS://SECURITE.INTRINSEC.COM/TAG/GESTION-DE-VULNERABILITES/) HACK IN PARIS (HTTPS://SECURITE.INTRINSEC.COM/TAG/HACK-IN-PARIS/) HASH (HTTPS://SECURITE.INTRINSEC.COM/TAG/HASH/) HIP (HTTPS://SECURITE.INTRINSEC.COM/TAG/HIP/) HTML5 (HTTPS://SECURITE.INTRINSEC.COM/TAG/HTML5/) HTTP (HTTPS://SECURITE.INTRINSEC.COM/TAG/HTTP/) INSOMNI'HACK (HTTPS://SECURITE.INTRINSEC.COM/TAG/INSOMNIHACK/) IPV6 (HTTPS://SECURITE.INTRINSEC.COM/TAG/IPV6/) ISSI (HTTPS://SECURITE.INTRINSEC.COM/TAG/ISSI/) NDH2K16 (HTTPS://SECURITE.INTRINSEC.COM/TAG/NDH2K16/) NDH2K17 (HTTPS://SECURITE.INTRINSEC.COM/TAG/NDH2K17/) NOSUCHCON (HTTPS://SECURITE.INTRINSEC.COM/TAG/NOSUCHCON/) OSSIR (HTTPS://SECURITE.INTRINSEC.COM/TAG/OSSIR/) OUTILS (HTTPS://SECURITE.INTRINSEC.COM/TAG/OUTILS/) PASSWORD (HTTPS://SECURITE.INTRINSEC.COM/TAG/PASSWORD/) PENTEST (HTTPS://SECURITE.INTRINSEC.COM/TAG/PENTEST/) RANSOMWARE (HTTPS://SECURITE.INTRINSEC.COM/TAG/RANSOMWARE/) RETOURS D'EXPÉRIENCE (HTTPS://SECURITE.INTRINSEC.COM/TAG/RETOURS-DEXPERIENCE/) REVERSE (HTTPS://SECURITE.INTRINSEC.COM/TAG/REVERSE/) RSSI TP (HTTPS://SECURITE.INTRINSEC.COM/TAG/RSSI-TP/) SENSIBILISATION (HTTPS://SECURITE.INTRINSEC.COM/TAG/SENSIBILISATION/) SOC (HTTPS://SECURITE.INTRINSEC.COM/TAG/SOC/) SSL (HTTPS://SECURITE.INTRINSEC.COM/TAG/SSL/) SSTIC (HTTPS://SECURITE.INTRINSEC.COM/TAG/SSTIC/) STHACK (HTTPS://SECURITE.INTRINSEC.COM/TAG/STHACK/) TABLEAU DE BORD (HTTPS://SECURITE.INTRINSEC.COM/TAG/TABLEAU-DE-BORD/) TABLEAUX DE BORD (HTTPS://SECURITE.INTRINSEC.COM/TAG/TABLEAUX-DE-BORD/) TABLEAUX DE BORD SÉCURITÉ (HTTPS://SECURITE.INTRINSEC.COM/TAG/TABLEAUX-DE-BORD-SECURITE/) TDB (HTTPS://SECURITE.INTRINSEC.COM/TAG/TDB/) TOIP (HTTPS://SECURITE.INTRINSEC.COM/TAG/TOIP/) VLAN (HTTPS://SECURITE.INTRINSEC.COM/TAG/VLAN/) VOIP (HTTPS://SECURITE.INTRINSEC.COM/TAG/VOIP/) WRITEUP (HTTPS://SECURITE.INTRINSEC.COM/TAG/WRITEUP/) XSS (HTTPS://SECURITE.INTRINSEC.COM/TAG/XSS/)

CATÉGORIES

Catégories Sélectionner une catégorie

ARCHIVES

Archives Sélectionner un mois