

25/10/2023



ASSURMER

Réalisation professionnelle n°10

*Mise en place d'une solution de
type Network Attached Storage*
Veille informationnelle

I. Veille informationnelle concernant la solution retenue

Afin de garantir la sécurité des données, il est nécessaire de mettre en place une veille informationnelle sur notre solution choisie.

Pour cela, nous avons choisi différents outils de veille afin d'être le plus au courant possible de l'actualité de TrueNAS, et être informé des vulnérabilités de celui-ci le plus rapidement possible après leur découverte.

Ces outils de veille sont :

- CertFR (<https://www.cert.ssi.gouv.fr>)
- La liste des CVE fournie par TrueNAS (<https://security.truenas.com/cves/>)
- Des flux RSS mis en place avec Inoreader (<https://www.inoreader.com/>)

Les flux RSS d'Inoreader ne trient pas les vulnérabilités par CVE mais nous permet d'être au courant de l'actualité plus globale autour de TrueNAS (nouvelles versions, fonctionnalités développées, etc.).

CertFr offre une liste des alertes de sécurité globale, elle permet de surveiller les vulnérabilités possibles des autres services de notre infrastructure :

ALERTES DE SÉCURITÉ

VULNÉRABILITÉ DANS APACHE STRUTS 2

 CERTFR-2023-ALE-013 • Publié le 13 décembre 2023 • **Alerte en cours**

Le 4 décembre 2023, Apache a publié un avis de sécurité concernant la vulnérabilité critique CVE-2023-50164 concernant le cadriciel Struts 2. Cette vulnérabilité permet à un attaquant non ...

[MÀJ] VULNÉRABILITÉ DANS CITRIX NETSCALER ADC ET NETSCALER GATEWAY

 CERTFR-2023-ALE-012 • Publié le 23 octobre 2023 • **Alerte en cours**

[Mise à jour du 22 novembre 2023]

L'éditeur a publié un document [3] le 20 novembre 2023 listant les différents journaux à analyser ainsi que les éléments à rechercher pour identifier une activité pouvant être liée à une ...

[MÀJ] MULTIPLES VULNÉRABILITÉS DANS CISCO IOS XE

 CERTFR-2023-ALE-011 • Publié le 17 octobre 2023 • **Alerte en cours**

[Mise à jour du 02 novembre 2023]

La version 17.3.8a est disponible.

[Mise à jour du 31 octobre 2023]

Enfin, pour avoir des informations plus précises sur TrueNAS, une liste des CVE récentes est donnée par TrueNAS, dont voici un extrait :

Known Issues

python v3.9.14

gh-97616 gh-97612 For more information see: <https://vuxml.FreeBSD.org/freebsd/d6d088c9-5064-11ed-bade-080027881239.html>

Note: iXsystems has determined that these vulnerabilities are not applicable to TrueNAS. This issue may be addressed in a future CORE 13.0 release.

squashfs-tools-4.3_1 – Integer overflow

CVE: CVE-2015-4645 For more info see: <https://vuxml.FreeBSD.org/freebsd/317487c6-85ca-11eb-80fa-14dae938ec40.html>

Note: iXsystems has determined that these vulnerabilities are not applicable to TrueNAS because the impacted utilities are not remotely accessible unless the system has already been compromised for remote root access. This issue may be addressed in a future TrueNAS release.

dnsmasq-2.86_2,1 – heap use-after-free in dhcp6_no_relay

CVE: CVE-2022-0934 For more info see: <https://vuxml.FreeBSD.org/freebsd/3f321a5a-b33b-11ec-80c2-1bb2c6a00592.html>

Note: iXsystems has determined that these vulnerabilities are not applicable to TrueNAS due to the lack of exposure of this utility. This issue may be addressed in a future TrueNAS release.

git-lite-2.34.1 – Multiple vulnerabilities

CVE: CVE-2022-39260 CVE: CVE-2022-39253 For more info see: <https://vuxml.FreeBSD.org/freebsd/2523bc76-4f01-11ed-929b-002590f2a714.html>

Note: iXsystems has determined that these vulnerabilities are not applicable to TrueNAS due to the lack of exposure of this utility. This issue may be addressed in a future TrueNAS release.