admin
Rapport de KRI Risque

192.168.10.7

Ce rapport présente les risques pricipales de list de serveur-rapport suivant:
192.168.10.7 - 2016-08-03 11:05:14 UTC

L'équipe de SecludIT est à votre disposition pour toute question.

Support Par SecludIT

Niveau de Risque Global

5.7

Elevé Risque

Niveau de Risque ANSSI

5.7

Elevé Risque

Access Control	Data Integrity	Malware	Outdated Software	Dos
5.2	5.7	0.0	0.0	0.0
Elevé	**Elevé**	**Aucun**	**Aucun**	**Aucun**

Référence: http://www.ssi.gouv.fr/guide/guide-dhygiene-informatique/

- Access Control - Contrôle d'Accès au server
- Data Integrity - Intégrité des données
- Malware - Logiciel Malveillant
- Outdated Software - Mise à Jour Logiciel
- Dos - Déni de Service

Niveau de Risque OWASP

5.7

Elevé Risque

OWASP A1 2013	OWASP A2 2013	OWASP A3 2013	OWASP A4 2013	OWASP A5 2013
0.0	3.6	0.0	0.0	4.3
Aucun	Mineur	Aucun	Aucun	Elevé

OWASP A6 2013	OWASP A7 2013	OWASP A8 2013	OWASP A9 2013	OWASP A10 2013
5.7	2.4	0.0	0.0	0.0
Elevé	Mineur	Aucun	Aucun	Aucun

Référence: https://www.owasp.org/index. php/Top_10_2013-Top_10

- A1 2013 - Injection
- A2 2013 - Broken Authentication and Session Management
- A3 2013 - Cross-Site Scripting
- A4 2013 - Insecure Direct Object References
- A5 2013 - Security Misconfiguration
- A6 2013 - Sensitive Data Exposure
- A7 2013 - Missing Function Level Access Control
- A8 2013 - Cross-Site Request Forgery
- A9 2013 - Using Components with Known Vulnerabilities
- A10 2013 - Unvalidated Redirects and Forwards

Compliance

Echoué

2.1	2.2.2	5.1.2	6.2	6.5
Passé	Passé	Passé	Passé	Echoué

Référence: https://www.pcisecuritystandards.org/document_library?document=pci_dss

- PCI-2.1 - Make sure that systems do not use vendor-supplied defaults
- PCI-2.2.2 - No unnecessary and insecure services and protocols running
- PCI-5.1.2 - No malware threats
- PCI-6.2 - System components and software have the latest patches installed. The use of vulnerability scoring is required to have no vuln with CVSS>4
- PCI-6.5 - Avoid common coding vulnerabilities