



Soluzioni Group

Report Summary

Executive Summary

 High Risk

The Executive Summary provides an overview of key findings with their severity information of the organization. Each part summarizes potential risk factors which must be addressed to prevent a potential breach.

Generated by

Dario Ayarza | dayarza@soluzioni.pe

Confidential: The following report contains confidential information. Do not distribute, email, fax, or transfer via any electronic mechanism unless it has been approved by the recipient company's security policy. All copies and backups of this document should be saved on protected storage at all times. Do not share any of the information contained within this report with anyone unless they are authorized to view the information. Violating any of the previous instructions is grounds for termination.

0-Days Summary

This data will be showed the percentage/proportional data by each category that provided next to the corresponding slice of pie (0-day family).

CVEs Summary

Organization top CVE

3325 Unique CVEs were found out of 255,966 CVEs entries



Filtered by: Servidores Cenares

⚡ High Risk CVE

ID	Count	Href
CVE-2024-6387	9	https://www.vicarius.io/vsociety/vulnerabilities/369435/CVE-2024-6387
CVE-2024-30064	3	https://www.vicarius.io/vsociety/vulnerabilities/367506/CVE-2024-30064
CVE-2024-30070	1	https://www.vicarius.io/vsociety/vulnerabilities/367500/CVE-2024-30070
CVE-2024-30062	4	https://www.vicarius.io/vsociety/vulnerabilities/367508/CVE-2024-30062
CVE-2024-30068	4	https://www.vicarius.io/vsociety/vulnerabilities/367502/CVE-2024-30068

⚡ Medium Risk CVE

ID	Count	Href
CVE-2024-30069	4	https://www.vicarius.io/vsociety/vulnerabilities/367501/CVE-2024-30069
CVE-2024-30067	4	https://www.vicarius.io/vsociety/vulnerabilities/367503/CVE-2024-30067
CVE-2024-30066	4	https://www.vicarius.io/vsociety/vulnerabilities/367504/CVE-2024-30066
CVE-2024-30065	4	https://www.vicarius.io/vsociety/vulnerabilities/367505/CVE-2024-30065
CVE-2024-30063	4	https://www.vicarius.io/vsociety/vulnerabilities/367507/CVE-2024-30063

⚡ Low Risk CVE

ID	Count	Href
CVE-2023-50868	4	https://www.vicarius.io/vsociety/vulnerabilities/352452/CVE-2023-50868
CVE-2023-42465	1	https://www.vicarius.io/vsociety/vulnerabilities/348089/CVE-2023-42465
CVE-2023-48231	24	https://www.vicarius.io/vsociety/vulnerabilities/345019/CVE-2023-48231
CVE-2023-3961	2	https://www.vicarius.io/vsociety/vulnerabilities/343754/CVE-2023-3961
CVE-2023-4154	3	https://www.vicarius.io/vsociety/vulnerabilities/344015/CVE-2023-4154

Filtered by: Servidores Cenares

xTags Summary

Dynamic exploit factors are being detected by exploitation tags (xTags). Each xTag designed to highlight unique factors across the entire organization, which may result in a potential breach.

Organization Top xTags

xTags Name	Affected Apps	Installed Assets
#has_patch	175	31
#attack_surface	56	33
#known_vulnerability	40	32
#availability_impact_if_exploited	32	31
#confidentiality_impact_if_exploited	33	32

Apps Summary

724 Installed Apps



Top 10 Risky Apps

ID	Versions	Assets	0-Day	CVE	Risk Level
PHP	1	1	878	342	High
Firefox	1	1	1003	0	High
Teamviewer	2	1	126	7	High
Openssl	3	18	458	42	High
Samba	2	3	0	62	High
SQL Server	8	6	7912	1	High
.NET	5	4	1	19	High
Python	3	14	110	5	High
Vim	1	12	0	145	High
Asp.net	5	2	305	0	High

Filtered by: Servidores Cenares



Assets Summary

35 Assets



Top 10 Risky Assets

ID	Internal IP	Apps	0-Day	CVE	Risk Level
SRVDBD01	192.168.11.10	29	14729	64	High
SRVDAPP01	192.168.11.20	22	7015	57	High
BARTON	192.168.10.191	22	16236	21	High
N6DBPRO1	192.168.10.69	25	28710	11	High
N6WSFS	192.168.10.64	162	616	114	High
N4DBDEV1	192.168.10.49	22	12560	2476	High
srvperp	192.168.10.178	271	4437	170	High
srvpfserp	192.168.10.179	225	4023	182	High
srvterp	192.168.11.178	271	4437	170	High
mad3nucleo	192.168.12.219	255	4494	50	High

Filtered by: Servidores Cenares