

1. Prezentare generală

Modulul VOGO eBS Vulnerability Management identifică, evaluează și raportează automat vulnerabilitățile de securitate ale infrastructurii informatice: servere Linux și Windows, servere web și aplicații web, servere de baze de date, firewall-uri și echipamente de rețea.

- ▶ **Produs integrat VOGO:** scannerul, baza de vulnerabilități, depozitul rezultatelor, consola și rapoartele funcționează ca un singur produs, cu o singură licență și un singur contract de suport.
- ▶ **Furnizare ca serviciu:** soluția este pusă la dispoziție ca serviciu pe toată durata contractului, cu feed-uri pentru organizații de tip enterprise.
- ▶ **Evaluare periodică:** scanări planificate, inclusiv trimestriale, cu istoricul tuturor rezultatelor.

2. Arhitectură și bibliotecile produsului

Modulul VOGO eBS Vulnerability Management rulează în infrastructura organizației și scanează fără agenți instalați pe dispozitivele scanate.

- ▶ **Componente:** scannerul de rețea, managerul scanărilor, baza de date a rezultatelor și consola web VOGO eBS.
- ▶ **Acces criptat:** consola și interfețele de administrare se accesează numai prin HTTPS.
- ▶ **Scalabilitate:** proiectat pentru medii complexe, cu un număr mare de dispozitive și scanări frecvente.
- ▶ **Biblioteci:** produsul folosește ca biblioteci open source mature: Greenbone OpenVAS.

3. Baza de vulnerabilități

Baza de vulnerabilități și exploit-uri cunoscute se actualizează automat, fără intervenție manuală, cel puțin zilnic.

- ▶ **Acoperire:** verificări pentru OS Security and Patch, Firewalls, DNS, FTP, SMTP, SNMP, LDAP, SMB, CGI, Web Servers, SQL Databases, Denial of Service și Default Accounts.
- ▶ **Scor CVSS:** fiecare vulnerabilitate are scorul CVSS (Common Vulnerability Scoring System) și este etichetată pe grade de risc: critică, ridicată, medie, scăzută.
- ▶ **KnowledgeBase:** pentru fiecare vulnerabilitate, natura riscului și recomandările de remediere.

4. Scanarea

Țintele se definesc ca adrese, game de adrese IP (range) și clase IP; fiecare scanare are configurația ei.

- ▶ **Configurare:** lista porturilor TCP și UDP, lista de vulnerabilități verificate, scanări cu sau fără autentificare pe diverse servicii, inclusiv brute force.
- ▶ **Scanare autentificată și neautentificată:** scanarea porturilor cu sau fără credențiale, auditul patch-urilor, auditul cu credențiale al configurațiilor pentru Windows, Unix și echipamente active de rețea, scanarea cu credențiale a unei largi palete de aplicații software.
- ▶ **Detecție:** servicii care rulează pe porturi non-standard, multiple instanțe ale aceluiași serviciu pe porturi diferite, dispozitive care nu răspund la ping.
- ▶ **Windows:** prin scanare autentificată se preiau utilizatorii, configurațiile de rețea, setările de registre, software-ul instalat, dispozitivele instalate și vulnerabilitățile.
- ▶ **Baze de date:** scanarea predefinită sau configurabilă a vulnerabilităților bazelor de date.
- ▶ **Aplicații web:** crawler-ul navighează automat prin toate paginile site-ului, evitând buclele circulare de link-uri, și detectează SQL injection, cross-site scripting (XSS), HTTP header injection, directory traversal, remote file inclusion și command execution.

5. Rezultate, rapoarte și integrare

Rezultatele scanărilor și evaluărilor se păstrează într-o bază de date, pentru raportare și istoric.

- ▶ **Stocare avansată:** volume mari de date de scanare, cu data descoperirii fiecărei vulnerabilități și ultima dată la care a fost observată, pentru filtrare și raportare în timp.

- **Funcționalități complexe:** căutare, filtrare, rapoarte personalizate, tendințele în timp și alerte automate.
- **Rapoarte detaliate:** rapoarte pe scorurile CVSS, pe servere și pe grade de risc, exportate în HTML, CSV și XML.
- **Integrare SIEM:** rezultatele se transmit componentei SIEM, pentru corelarea cu celelalte evenimente de securitate.
- **Plan de remediere:** riscurile se clasifică și se însoțesc de recomandări, validate de experții de evaluare a vulnerabilităților.

6. Licențiere și suport

- Modulul VOGO eBS Vulnerability Management se furnizează ca serviciu, pe toată durata contractului.
- **Support:** pe perioada contractului, cu actualizarea bazei de vulnerabilități și acces direct la producător pentru deschiderea cazurilor de suport.
 - **Servicii:** configurarea scanărilor la punerea în producție și evaluarea periodică pe toată perioada de garanție.

7. Capturi de ecran din VOGO eBS

Capturile de mai jos sunt făcute în paginile VOGO eBS ale produsului.

COMPANIA DE APĂ

Favorites

Home

Recente

Notificări

Operațiuni azi

Politici și proceduri

Servicii digitale angajați

Ajutor & Suport

Setări

Administrator APA...

VOGO eBS Vulnerability Manage

Căutare globală...

Ctrl + K

Managementul vulnerabilităților — servere scanate, vulnerabilități și corecții

4

199

16

98

123 / 24

105

Servere scanate

Serverul	Sistemul de operare	Pachete	Critice	Ridicate	Medii	Scăzute	Ultima scanare
Server baze de date — analiză	Debian GNU/Linux 12 (bookworm)	97	16	98	123	24	2026-10-11 18:58
Server baze de date — registratură	Alpine Linux v3.24	44	0	0	0	0	2026-10-11 18:58
Agent de monitorizare	Alpine Linux v3.24	40	0	0	0	0	2026-10-11 18:58
Proxy invers — portal	Alpine Linux v3.24	18	0	0	0	0	2026-10-11 18:58

Vulnerabilitățile cele mai grave

Vulnerabilitatea	Serverul	Pachetul	Versiunea instalată	Versiunea corectată	CVSS	Severitatea
CVE-2019-1010022	Server baze de date — analiză	glibc	2.36-9+deb12u13	fără corecție publicată	9,8	Critică
CVE-2026-5450	Server baze de date — analiză	glibc	2.36-9+deb12u13	fără corecție publicată	9,8	Critică
CVE-2026-42010	Server baze de date — analiză	gnutls28	3.7.9-2+deb12u6	3.7.9-2+deb12u7	9,8	Critică
CVE-2026-6653	Server baze de date — analiză	libxml2	2.9.14+dfsg-1.3~deb12u5	fără corecție publicată	9,8	Critică
CVE-2026-57433	Server baze de date — analiză	perl	5.36.0-7+deb12u3	5.36.0-7+deb12u4	9,8	Critică
CVE-2026-8376	Server baze de date — analiză	perl	5.36.0-7+deb12u3	5.36.0-7+deb12u4	9,8	Critică
CVE-2023-45653	Server baze de date — analiză	zlib	1:1.2.13.dfsg-1	fără corecție publicată	9,8	Critică
CVE-2026-33845	Server baze de date — analiză	gnutls28	3.7.9-2+deb12u6	3.7.9-2+deb12u7	9,1	Critică

VOGO® eBS ECM

Enterprise Business Solutions

© 2026 VOGO — Toate drepturile rezervate. Confidențialitate Termeni și condiții

VOGO eBS Vulnerability Management Console: indicatorii ultimei scanări, serverele scanate și vulnerabilitățile

Servere scanate							
Serverul	Sistemul de operare	Pachete	Critice	Ridicate	Medii	Scăzute	Ultima scanare
Server baze de date — analiză	Debian GNU/Linux 12 (bookworm)	97	16	98	123	24	2026-10-11 18:58
Server baze de date — registratură	Alpine Linux v3.24	44	0	0	0	0	2026-10-11 18:58
Agent de monitorizare	Alpine Linux v3.24	40	0	0	0	0	2026-10-11 18:58
Proxy invers — portal	Alpine Linux v3.24	18	0	0	0	0	2026-10-11 18:58

Serverele scanate, cu sistemul de operare, pachetele verificate și vulnerabilitățile pe grade de risc

Vulnerabilitățile cele mai grave						
Vulnerabilitatea	Serverul	Pachetul	Versiunea instalată	Versiunea corectată	CVSS	Severitatea
CVE-2019-1010022	Server baze de date — analiză	glibc	2.36-9+deb12u13	fără corecție publicată	9,8	Critică
CVE-2026-5450	Server baze de date — analiză	glibc	2.36-9+deb12u13	fără corecție publicată	9,8	Critică
CVE-2026-42010	Server baze de date — analiză	gnutls28	3.7.9-2+deb12u6	3.7.9-2+deb12u7	9,8	Critică
CVE-2026-6653	Server baze de date — analiză	libxml2	2.9.14+dfsg-1.3~deb12u5	fără corecție publicată	9,8	Critică
CVE-2026-57433	Server baze de date — analiză	perl	5.36.0-7+deb12u3	5.36.0-7+deb12u4	9,8	Critică
CVE-2026-8376	Server baze de date — analiză	perl	5.36.0-7+deb12u3	5.36.0-7+deb12u4	9,8	Critică
CVE-2023-45853	Server baze de date — analiză	zlib	1:1.2.13.dfsg-1	fără corecție publicată	9,8	Critică
CVE-2026-33845	Server baze de date — analiză	gnutls28	3.7.9-2+deb12u6	3.7.9-2+deb12u7	9,1	Critică
CVE-2026-88647	Server baze de date — analiză	gnutls28	3.7.9-2+deb12u6	fără corecție publicată	9,1	Critică
CVE-2026-95210	Server baze de date — analiză	gnutls28	3.7.9-2+deb12u6	fără corecție publicată	9,1	Critică
CVE-2026-34182	Server baze de date — analiză	openssl	3.0.19-1~deb12u2	3.0.20-1~deb12u2	9,1	Critică
CVE-2026-75803	Server baze de date — analiză	openssl	3.0.19-1~deb12u2	3.0.22-1~deb12u1	9,1	Critică
CVE-2026-12087	Server baze de date — analiză	perl	5.36.0-7+deb12u3	5.36.0-7+deb12u4	9,1	Critică
CVE-2026-13221	Server baze de date — analiză	perl	5.36.0-7+deb12u3	5.36.0-7+deb12u4	9,1	Critică
CVE-2026-42496	Server baze de date — analiză	perl	5.36.0-7+deb12u3	5.36.0-7+deb12u4	9,1	Critică
CVE-2025-7458	Server baze de date — analiză	sqlite3	3.40.1-2+deb12u2	fără corecție publicată	9,1	Critică
CVE-2019-1010023	Server baze de date — analiză	glibc	2.36-9+deb12u13	fără corecție publicată	8,8	Ridicată
VOGO® eBS ECM Enterprise Business Solutions © 2026 VOGO — Toate drepturile rezervate. Confidențialitate Termeni și condiții						

Vulnerabilitățile cele mai grave: scorul CVSS, versiunea instalată și versiunea corectată