PREGLED POSTUPKA #104708

1 PODACI O NARUČIOCU

Naziv naručioca	AGENCIJA ZA SPREČAVANJE KORUPCIJE
PIB	11006507
E-mail	kabinet@antikorupcija.me
Telefon	020/447-702, 202/447-723
Internet adresa	www.antikorupcija.me
Fax	020/234-082
Adresa	Ulica Kralja Nikole 27/V
Grad	Podgorica
Poštanski broj	81000

2 OSNOVNI PODACI

Opis predmeta javne nabavke	Softver za otkrivanje ranjivosti
Status	U toku
Vrsta predmeta	Usluge
Vrsta postupka	Jednostavna nabavka
Službenik za javne nabavke	Dragana Dacić
Kontakt	020-447-718
Datum objave	04.12.2025. 13:10
Napomena	-

3 FAZE U POSTUPKU

Vrsta faze	Opis	Početak podnošenja	Kraj podnošenja	Datum otvaranja	Status
Zahtjev za podnošenje ponuda	Zahtjev za podnošenje ponuda - Softver za otkrivanje ranjivosti	04.12.2025 13:10	08.12.2025 10:30	08.12.2025 10:30	U toku

4 DODATNE INFORMACIJE

Predmet javne nabavke se nabavlja	kao cjelina
Posebni oblici javne nabavke	
Okvirni sporazum	Ne
Dinamički sistem nabavki	Ne
Elektronska aukcija	Ne
Elektronski katalog	Ne
Nabavka se sprovodi kao	
Zajednička nabavka	Ne
Centralizovana nabavka	Ne
Nabavka je	
Zelena	Ne
Društveno odgovorna	Ne

5 STAVKE PLANA

Godina	Opis	Vrijednost nabavke	Vrijednost PDV	Okvirni sporazum	Vrijednost OS	Vrijednost PDV OS	Vrsta postupka
2025	**AGENCIJA ZA SPREČAVANJE KORUPCIJE** **Softver za otkrivanje ranjivosti** 48732000 - Softverski paket za bezbjednost podataka	12.000,00 EUR	2.520,00 EUR	-	-	-	Jednostavna nabavka

6 USLOVI ZA UČEŠĆE U POSTUPKU I ZAHTJEVI U POGLEDU NAČINA IZVRŠAVANJA PREDMETA NABAVKE

Opis	Tip uslova / zahtjeva
Uz ponudu se dostavlja Izjava ponuđača o ispunjenosti uslova utvrđenih zahtjevom i nepostojanju sukoba interesa, potpisana od strane ovlašćenog lica ponuđača, data na Obrascu 2, preuzimanjem na posebnom aplikativnom dijelu elektronskog sistema javnih nabavki, shodno članu 9 stav 10 Pravilnika o načinu sprovođenja jednostavnih nabavki („Službeni list CG“, br. 16/23, 20/23, 36/23, 114/23, 49/24 i 114/24)	Obrazac 2
Mjesto izvršenja ugovora je sjedište Agencije za sprečavanje korupcije, Ulica Kralja Nikole 27/V, Podgorica	Mjesto izvršenja ugovora
Rok važenja ponude: 60 dana od dana otvaranja ponuda	Rok važenja ponude
Način plaćanja: virmanski, na žiro račun Izvršioca. Žiro račun:_____ Banka:_____ (Ponuđač je obavezan navesti broj žiro računa i banke).	Način plaćanja
Rok za isporuku sistema ne smije biti duži od 10 dana od dana potpisivanja ugovora	Rok izvršenja ugovora
Sprovođenje kontrole kvaliteta vršiće službenici Odsjeka za informacione tehnologije Agencije.	Način sprovođenja kontrole kvaliteta
Plaćanje će se vršiti u roku do 30 dana nakon dostavljanja fakture i potpisivanja zapisnika o isporuci sistema koji će potpisati predstavnici naručioca i izvršioca. Uredno ispostavljena faktura i zapisnik o isporuci sistema potpisan od strane predstavnika Naručioca i Izvršioca predstavlja osnov za plaćanje ugovorene cijene Rok plaćanja	Rok plaćanja

7 KRITERIJUMI ZA IZBOR NAJPOVOLJNIJE PONUDE

Opis
Cijena

8 PREDMET NABAVKE

Procijenjena vrijednost nabavke: **12.000,00 EUR**

TEHNIČKA SPECIFIKACIJA PREDMETA NABAVKE

	Opis predmeta nabavke	Bitne karakteristike predmeta nabavke	Količina
		1. Predmet nabavke Predmet nabavke je nabavka, instalacija, konfiguracija i puštanje u rad OpenVAS sistema za skeniranje ranjivosti informaciono-komunikacione infrastrukture naručioca, uključujući: • Greenbone Community Edition (GCE) • OpenVAS Scanner • Greenbone Vulnerability Manager (GVMD) • Security Assistant (SA WEB UI) • Notus Scanner • Greenbone Feeds (NVT, SCAP, CERT) • PostgreSQL bazu podataka • Kompletno virtuelizovano okruženje Sistem mora biti instaliran on-premise, unutar infrastrukture naručioca, bez ikakvog eksternog slanja podataka. 2. Zahtijevani softver i platforma Nabavljeni sistem mora biti baziran isključivo na: 2.1. Greenbone Community Edition (GCE) Verzija: najnovija stabilna u trenutku implementacije	

Komponente:
• GSA – Greenbone Security Assistant (web interfejs)
• GVMD – Greenbone Vulnerability Manager
• OpenVAS Scanner
• Notus Scanner
• Greenbone Feed Sync

Deployment model: Linux deployment po preporuci proizvođača

2.2. OpenVAS Scanner
• Skeniranje mrežnih ranjivosti
• Autentifikovani i neautentifikovani skenovi
• Podrška za skeniranje preko SSH i SMB protokola
• Podrška za TCP i UDP protokole
• Upotreba kompletnih NVT (Network Vulnerability Tests) feedova

2.3. Greenbone Feeds
Ponuđač mora obezbijediti integraciju sledećih feedova:
• NVT Feed – testovi ranjivosti
• SCAP Feed – OVAL/CPE/CVE/ konfiguracione baze
• CERT Feed – advisories i sigurnosna upozorenja
• Automatska dnevna sinhronizacija feedova
• Offline feed update opcija (po potrebi naručioca)

2.4. PostgreSQL
• Baza podataka za GVMD
• Automatsko kreiranje šema
• Podešavanje optimizacije (autovacuum, indexing)

3. Funkcionalni zahtjevi
Sistem mora omogućiti sve funkcije dostupne u OpenVAS/GCE okruženju:

3.1. Upravljanje skenovima (GVMD)
• Kreiranje ciljeva (Targets)
• Upravljanje port listama
• Upravljanje credentialima za autentifikovane preglede
• Sken konfiguracije (Full and Fast, Full and Fast Ultimate, Host Discovery, System Discovery, itd.)
• Upravljanje taskovima (Tasks), zakazivanje i izvršavanje

3.2. Security Assistant (SA) – Web UI
• HTTPS web interfejs
• Vizuelizacija rezultata skeniranja
• Analiza ranjivosti po CVSS v3 skoru
• Pregled statusa feedova
• Upravljanje korisnicima i rolama
• Izvoz izvještaja u: PDF, HTML, CSV, XML, JSON

3.3. OpenVAS skeniranje ranjivosti
• Detekcija ranjivosti po CVE bazi
• Detekcija ranjivih verzija servisa i operativnih sistema
• Identifikacija konfiguracionih grešaka
• Skeniranje mrežnih servisa (SSH, RDP, SMB, HTTP/HTTPS, SQL serveri, VoIP, SNMP, DNS, itd.)
• Skeniranje Web aplikacija i web servisa kroz HTTP(S) plugin bazu NVT testova

Autentifikovani skenovi:
• Windows (SMB, WinRM)

		• Linux (SSH) 4. Izvještavanje (Reporting) Sistem mora omogućiti generisanje izvještaja iz platforme: • Izvještaji po tipu ranjivosti • Izvještaji po kritičnosti (Severity / CVSS v3) • Izvještaji po hostovima, mrežnim opsezima i poslovnim cjelinama • Trend analiza (ponovljena skeniranja i uporedni izvještaji) Izvoz u formate: • PDF • HTML • CSV • XML • JSON 5. Arhitektura rješenja Ponuđač mora isporučiti sistem u sljedećoj arhitekturi: 5.1. Servisi • openvas-scanner servis • gvmd manager servis • sa web UI servis • notus-scanner servis • redis-server za keširanje i komunikaciju • postgresql DB servis 5.2. Deployment • Preferirano: Docker Compose deployment (preporuka	
1	Softver za otkrivanje ranjivosti		1,00 komplet

Greenbone-a)
• Alternativa: instalacija na Linux server (Ubuntu/Debian) uz zvanična uputstva

5.3. Sistem se instalira na infrastrukturu naručioca
• Bez cloud komponenata
• Bez eksternog slanja podataka
• Bez telemetrije i remote logging-a

6. Hardversko–sistemski zahtjevi
Naručilac će obezbijediti virtuelnu mašinu minimalne specifikacije servera:
• 4 CPU jezgra
• 8 GB RAM (preporučeno 12–16 GB)
• 80 GB SSD prostora
• Linux OS (Ubuntu 22.04/24.04 ili Debian 12)
• Pristup svim mrežnim segmentima koji se skeniraju

7. Bezbijednosni zahtjevi
Sistem mora ispuniti:
• HTTPS pristup SA web interfejsu
• Enkripciju komunikacije između komponenti (GVMD–OpenVAS–GSA–PostgreSQL)
• Evidenciju logova svih aktivnosti korisnika
• Internu izolaciju preko Docker network-a ili Linux ACL-ova
• Nema slanja rezultata na internet, cloud ili eksternim servisima

8. Aktivnosti ponuđača (obavezne)
Ponuđač mora obaviti kompletan posao implementacije:
• Analiza i planiranje implementacije

		• Instalacija kompletnog OpenVAS okruženja • Konfiguracija GVMD, SA i OpenVAS skenera • Sinhronizacija feedova i provjera integriteta • Kreiranje početnih “Targets”, “Port Lists”, “Scan Configs” i “Tasks” • Izvođenje probnog skeniranja • Optimizacija skeniranja (Throttle, Max Hosts, Max Checks) • Izrada kompletne dokumentacije • Obuka administratora naručioca • Primopredaja sistema i verifikacija funkcionalnosti 9. Obuka naručioca Obuka mora obuhvatiti: • Uvod u OpenVAS arhitekturu • Kreiranje i upravljanje skenerskim zadacima • Rad sa SA web interfejsom • Analiza izvještaja i CVSS metodologije • Autentifikovani skenovi (SSH/SMB) • Održavanje sistema i backup procedura 10. Očekivani rezultat Po okončanju implementacije naručilac dobija: • Potpuno funkcionalan OpenVAS sistem • Kontinuirano ažurirane vulnerability feedove • Potpuni uvid u ranjivosti svoje infrastrukture • Sistem za izvještavanje spreman za revizije i bezbjednosne kontrole • Obučeno osoblje • Dokumentovan i operativan sistem	