



appsec

Report

Vulnerability scan systému 127.0.0.1

Dokument je duševním vlastnictvím společnosti APPSEC s.r.o.. Dispoziční právo k dokumentu náleží společnosti Example Company. Bez souhlasu autora je zakázáno dokument reprodukovat, publikovat nebo jinak používat k libovolným účelům mimo projekt Vulnerability scan systému 127.0.0.1. A to ani v částech ani v celku. Nakládání s dokumentem se řídí zákonem č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů, v aktuálním znění.

Obsah

1	Úvod	3
1.1	Disclaimer	3
2	Klasifikace zranitelností	4
2.1	Podle míry závažnosti	4
3	Výsledky penetračního testu	5
3.1	Identifikované zranitelnosti	5
3.1.1	Nepodporovaný operační systém ■	6
3.1.2	Zranitelná verze Apache serveru ■	7
3.1.3	Apache HTTP Server Byte Range DoS ■	8
3.1.4	NFS shares jsou čitelné bez omezení ■	9
3.1.5	OpenSSH MaxAuthTries Bypass ■	10
3.1.6	SMB sdílené disky přístupné ■	11
3.1.7	Chybí HSTS ■	12
3.1.8	FTP zapisovatelné anonymnímu uživateli ■	13
3.1.9	Nedůvěryhodný SSL certifikát ■	14
3.1.10	OpenSSL 'ChangeCipherSpec' MiTM zranitelnost ■	15
3.1.11	Podporováno SSL3, možný útok POODLE ■	16
3.1.12	POP3 - STLS Plaintext Command Injection ■	17
3.1.13	Dostupné anonymní FTP ■	18
3.1.14	Podporovány RC4 šifry ■	19
3.1.15	Použitý telnet ■	20
3.1.16	SSL podporovány středně slabé šifry ■	21
3.1.17	Únik informací z hlaviček webového serveru ■	22

1 Úvod

1.1 Disclaimer






Vulnerability scan slouží k prvotnímu zběžnému posouzení bezpečnosti scanovaného serveru. V případě vulnerability scanu nedochází, narozdíl od penetračního testu, k ověřování nalezených zranitelností a ručnímu hledání zranitelností. Z tohoto důvodu je pravděpodobné, že ve výsledcích z vulnerability scanu se může nacházet určité množství tzv. false positive, což jsou nálezy, které se ve skutečnosti na serveru nenacházejí. Zároveň je velice pravděpodobné, že při vulnerability scanu nebyly nalezeny všechny zranitelnosti, které se na serveru nacházejí.

2 Klasifikace zranitelností

V této kapitole je popsána klasifikace jednotlivých nalezených zranitelností. Každé zranitelnosti je přiřazena míra závažnosti podle dopadů, které by zneužití dané chyby mělo na testovaný systém.

2.1 Podle míry závažnosti

Závažnost jednotlivých nálezů vychází z jejich dopadů na celkové zabezpečení systému. Během hodnocení závažnosti jednotlivých nálezů je zohledněno případné využití společně s ostatními nalezenými zranitelnostmi.

- Kritická 
Závažná zranitelnost, která má přímé dopady na celkovou bezpečnost testovaného systému.
- Vysoká 
Zranitelnost, která může mít přímé dopady na bezpečnost testovaného systému v případě schopného či motivovaného útočníka.
- Střední 
Zranitelnost, která sama o sobě nemá dopad na celkovou bezpečnost testovaného systému, nicméně společně s dalšími zranitelnostmi může představovat určité riziko.
- Nízká 
Nález, který má nízký dopad na celkovou bezpečnost testovaného systému, jedná se většinou spíše o best practices.
- Informativní 
Nález, který je čistě informativní povahy a nepředstavuje bezpečnostní problém.

3 Výsledky penetračního testu

V této kapitole uvádíme technické informace k provedenému vulnerability scanu.

3.1 Identifikované zranitelnosti

V této kapitole jsou uvedeny jednotlivé zranitelnosti a nálezy seřazené podle závažnosti od nejzávažnějších po nejméně závažné. Jedná se o nálezy, které byly identifikovány během vulnerability scanu. Jsou zde uvedeny společně s případnými dopady a doporučením na eliminaci rizika. Vzhledem k povaze vulnerability scanu nemusí být jejich seznam kompletní. V případě nalezených zranitelností tedy doporučujeme věnovat danému problému pozornost a opravit daný typ zranitelnosti v celém systému.

3.1.1 Nepodporovaný operační systém ■

Závažnost: Ovlivněné systémy:

- IP - num_port/tcp.udp
- IP - num_port/tcp.udp
- IP - num_port/tcp.udp

Nález

Během testu bylo zjištěno, že na serveru běží stará, již nepodporovaná verze operačního systému. Jedná se o následující operační systém v dané verzi: - OS, verze

Riziko

Z důvodu již nedostupné podpory pro danou verzi operačního systému nejsou nově nalezené bezpečnostní zranitelnosti opravovány. V případě, že je nalezena nějaká závažná bezpečnostní chyba, její oprava nebude systému dostupná běžnými prostředky (aktualizační mechanismus), což povede ke zranitelnosti daného systému a dříve či později k jeho kompromitaci.

Doporučení

Doporučujeme aktualizaci na nejnovější podporovanou verzi operačního systému.

3.1.2 Zranitelná verze Apache serveru ■

Závažnost: Ovlivněné systémy:

- IP - num_port/tcp.udp
- IP - num_port/tcp.udp
- IP - num_port/tcp.udp

Nález

Během penetračního testu bylo zjištěno, že na daných systémech je provozován webový server Apache ve zranitelné verzi 2.4.XX. Na danou zranitelnost existuje veřejně dostupný a jednoduše použitelný RCE exploit.

Riziko

Zneužitím této zranitelnosti může být útočník schopen docílit spuštění libovolného kódu na zranitelném systému pod právy uživatele se kterými webový server běží.

Doporučení

Doporučujeme aktualizovat webový server na nejnovější podporovanou verzi.

3.1.3 Apache HTTP Server Byte Range DoS ■

Závažnost: Ovlivněné systémy:



- IP - num_port/tcp.udp
- IP - num_port/tcp.udp
- IP - num_port/tcp.udp

Nález

Během testu bylo zjištěno, že na daném serveru běží verze apache webového serveru, která je zranitelná útokem zvaným Server Byte Range odepření služby.

Riziko

Posláním několika HTTP požadavků s přesahujícími hodnotami v Range a Request-Range hlavičkách požadavku může vést k vyčerpání paměti a procesorového času. Vzdálený neautentizovaný uživatel je tímto způsobem schopný provést DoS útok na webový server.

Doporučení

Doporučujeme aktualizovat na Apache verze 2.2.21 nebo novější. Případně je možné použít workaround dostupný u CVE-2011-3192.

3.1.4 NFS shares jsou čitelné bez omezení ■

Závažnost: Ovlivněné systémy:

- IP - num_port/tcp.udp
- IP - num_port/tcp.udp
- IP - num_port/tcp.udp

Nález

Během penetračního testu bylo zjištěno, že exportované NFS Shares jsou připojitelné a čitelné odkudkoliv. Ačkoliv se na serveru 127.0.0.1 v exportovaných discích nachází pouze dva symbolické odkazy, tak je na něm možné vytvářet nová data.

[...snipo...]

Riziko

Rizikem je například zneužití dostupných dat (jsou-li). Dále také možnost, že útočník zneužije dostupné diskové kapacity k ukládání obsahu, i nelegálního.

Doporučení

Doporučujeme na firewallu omezit IP adresy ze kterých jsou sdílená data přístupná. Také doporučujeme zvážení provozování NFS v případě, že není nutné nebo se dá nahradit bezpečnější alternativou.

3.1.5 OpenSSH MaxAuthTries Bypass ■

Závažnost: Ovlivněné systémy:



- IP - num_port/tcp.udp
- IP - num_port/tcp.udp
- IP - num_port/tcp.udp

Nález

Během testu bylo zjištěno, že v použité verzi SSH se nachází zranitelnost umožňující útočníkovi podvrhnutí řetězce 'devices' a tím obejít nastavení parametru MaxAuthTries, který omezuje maximální počet pokusů o přihlášení k SSH serveru.

Riziko

Tato zranitelnost umožňuje útočníkovi neomezeně hádat heslo k uživatelskému účtu a provést tzv. brute force útok, případně dostat server do stavu odepření služby.

Doporučení

Doporučujeme aktualizovat OpenSSH server na verzi 7.0 nebo novější.

3.1.6 SMB sdílené disky přístupné ■

Závažnost: Ovlivněné systémy:



- IP - num_port/tcp.udp
- IP - num_port/tcp.udp
- IP - num_port/tcp.udp

Nález

Během penetračního testu bylo zjištěno, že některé exportované SMB sdílené disky jsou připojitelné a čitelné odkudkoliv. Konkrétně se jedná o 'inst' a 'default'.

Riziko

Rizikem je možnost úniku potenciálně citlivých dat. Dále také možnost, že útočník zneužije dostupné diskové kapacity k ukládání obsahu, i nelegálního.

Doporučení

Doporučujeme na firewallu omezit IP adresy ze kterých jsou sdílená data přístupná, a především nepovolovat anonymní/guest přístup k datům. Také doporučujeme zvážení provozování SMB v případě, že není nutné nebo se dá nahradit bezpečnější alternativou.

3.1.7 Chybí HSTS ■

Závažnost: Ovlivněné systémy:



- IP - num_port/tcp.udp
- IP - num_port/tcp.udp
- IP - num_port/tcp.udp

Nález

Během testů bylo zjištěno, že webový server nevynucuje HTTP Strict Transport Security (HSTS). Jedná se o mechanismus chráníci komunikaci před downgrade útoku a únosem spojení.

Riziko

V případě chybějící HSTS hlavičky může být útočník schopen provést downgrade útoky na šifrované spojení, SSL stripping útok, man in the middle útoky a další.

Doporučení

Doporučujeme nastavení HSTS hlaviček Strict-Transport-Security na webovém serveru.

3.1.8 FTP zapisovatelné anonymnímu uživateli ■

Závažnost: **Ovlivněné systémy:**



- IP - num_port/tcp.udp
- IP - num_port/tcp.udp
- IP - num_port/tcp.udp

Nález

Během penetračního testu bylo zjištěno, že některé z adresářů na uvedených FTP serverech jsou zapisovatelné pro anonymního uživatele.

Riziko

Zapisovatelné adresáře na FTP serveru mohou být zneužity například pro anonymní vyměňování nelegálního obsahu, například malwaru nebo pornografie. Uživatel také může být schopen, nahráním velkých souborů, zahltit FTP server a znemožnit nahrávání dalších, i legitimních, souborů.

Doporučení

Doporučujeme nastavit FTP server tak, aby neumožňoval anonymním uživatelům zapisování do žádných z adresářů.

3.1.9 Nedůvěryhodný SSL certifikát ■

Závažnost: **Ovlivněné systémy:**



- IP - num_port/tcp.udp
- IP - num_port/tcp.udp
- IP - num_port/tcp.udp

Nález

Bylo zjištěno, že na serveru www.example.com je použit certifikát platný pouze pro doménu mail.example.com

Riziko

Používání certifikátu pro jinou doménu snižuje důvěryhodnost a tím i bezpečnost šifrovaného spojení.

Doporučení

Doporučujeme vygenerování a používání certifikátu určeného pro danou doménu.

3.1.10 OpenSSL 'ChangeCipherSpec' MiTM zranitelnost ■

Závažnost: Ovlivněné systémy:



- IP - num_port/tcp.udp
- IP - num_port/tcp.udp
- IP - num_port/tcp.udp

Nález

Během testu bylo zjištěno, že použitá verze OpenSSL obsahuje zranitelnost man-in-the-middle známou jako ChangeCipherSpec. Jedná se o zranitelnost způsobenou reakcí na speciálně provedený handshake.

Riziko

Tato zranitelnost může útočníkovi umožnit dešifrovat nebo podvrhnout SSL zprávu tím způsobem, že je serveru řečeno aby zašifroval komunikaci ještě před výměnou klíče, čímž dochází k použití predikovatelných klíčů což umožňuje útočníkovi dešifrování potenciálně citlivých informací.

Doporučení

Doporučujeme aktualizovat OpenSSL na verzi 1.0.0m / 1.0.1h nebo novější.

3.1.11 Podporováno SSL3, možný útok POODLE ■

Závažnost: Ovlivněné systémy:

- IP - num_port/tcp.udp
- IP - num_port/tcp.udp
- IP - num_port/tcp.udp

Nález

V průběhu penetračního testu byla na daném serveru a dané službě zjištěna zranitelnost POODLE (Padding Oracle On Downgraded Legacy Encryption). Jedná se o man-in-the-middle information disclosure útok umožňující útočnickovi dešifrování vybraného bytu ciphertextu.

Riziko

V případě úspěšného útoku POODLE může být útočník schopen dešifrovat šifrovanou komunikaci. Toto může vést k úniku citlivých informací jako například přihlašovací údaje, session cookies či jakékoliv jiné citlivé informace, které se mohou mezi aplikací a uživatelem přenášet.

Doporučení

Jedná se o zranitelnost, která je principiální pro SSLv3, nikoliv pro konkrétní implementaci. Doporučujeme tedy zakázání SSLv3 na úrovni konfigurace daného serveru a používání pouze TLSv1.1 nebo vyšší verze. V serveru nginx toho lze dosáhnout například použitím direktivy `ssl_protocols TLSv1.2 TLSv1.1;`, která povolí pouze bezpečné TLS verze 1.1 a 1.2.

3.1.12 POP3 - STLS Plaintext Command Injection ■

Závažnost: Ovlivněné systémy:

- IP - num_port/tcp.udp
- IP - num_port/tcp.udp
- IP - num_port/tcp.udp

Nález

Během penetračního testu bylo zjištěno, že pop3 server je náchylný na command injection v průběhu domluvy šifrovaného komunikačního kanálu.

Při poslání následujícího paketu:

```
STLS\r\nCAPA\r\n
```

Došlo k následující odpovědi ze serveru:

```
+OK Begin TLS negotiation  
+OK Capability list follows
```

Riziko

Zranitelnost umožňuje neautentizovanému útočníkovi injektování příkazů v plaintext fázi tak, aby byly spuštěny v ciphertext fázi.

Doporučení

Doporučujeme aktualizovat POP3 server na nejnovější podporovanou verzi.

3.1.13 Dostupné anonymní FTP ■

Závažnost: **Ovlivněné systémy:**



- IP - num_port/tcp.udp
- IP - num_port/tcp.udp
- IP - num_port/tcp.udp

Nález

Na daný ftp server je možné se přihlásit jako anonymní uživatel. Riziko je sníženo tím, že nejsou na daných serverech dostupná citlivá data. A také není možné data na dané servery nahrávat anonymním uživatelům.

Riziko

Rizikem takového nastavení je možnost, že na daný server budou omylem nahrána citlivá data, která pak budou dostupná všem, včetně případného útočníka, který by mohl data zneužít.

Doporučení

Doporučujeme zvážit nutnost použití anonymního ftp serveru pro sdílení dat.

3.1.14 Podporovány RC4 šifry ■

Závažnost: Ovlivněné systémy:

- IP - num_port/tcp.udp
- IP - num_port/tcp.udp
- IP - num_port/tcp.udp

Nález

Během penetračního testu bylo zjištěno, že webový server na kterém běží testovaná aplikace podporuje cipher suites, které používají RC4 šifry. Jedná se o následující cipher suites:

TLS_ECDHE_RSA_WITH_RC4_128_SHA

TLS_RSA_WITH_RC4_128_SHA

Riziko

Algoritmus RC4 nekorektně pracuje se stavovými daty a klíčem během inicializační fáze. Toto může umožnit útočníkovi provést útok, který může vést k získání potenciálně citlivých informací.

Doporučení

Doporučujeme v konfiguraci webového serveru vypnout podporu pro dané cipher suites.

3.1.15 Použitý telnet ■

Závažnost: Ovlivněné systémy:

- IP - num_port/tcp.udp
- IP - num_port/tcp.udp
- IP - num_port/tcp.udp

Nález

Na serveru běží telnet, který nepoužívá žádnou formu šifrování. Toto není doporučeno, jelikož přenášená data mohou být útočníkem zachycena při přenosu po síti.

Riziko

Riziko tohoto nálezu je sníženo tím, že telnet server okamžitě po připojení spojení ukončí. Je tedy pravděpodobně nasazena nějaká forma filtrování klientů podle IP adres. Doporučujeme prověřit, jestli není nastavení filtru příliš obecné.

Doporučení

Místo protokolu telnet doporučujeme pro veškerou vzdálenou administraci zařízení používat protokol SSH-2, který díky použití kryptografie poskytuje dostatečnou ochranu přenášených dat.

3.1.16 SSL podporovány středně slabé šifry ■

Závažnost: Ovlivněné systémy:

- IP - num_port/tcp.udp
- IP - num_port/tcp.udp
- IP - num_port/tcp.udp

Nález

Během testu bylo zjištěno, že daná služba na dané adrese podporuje středně slabé šifry. Jedná se o následující šifry:

SSLv2

DES-CBC-MD5 Kx=RSA Au=RSA Enc=DES-CBC(56) Mac=MD5

TLSv1

EDH-RSA-DES-CBC-SHA Kx=DH Au=RSA Enc=DES-CBC(56) Mac=SHA1

ADH-DES-CBC-SHA Kx=DH Au=None Enc=DES-CBC(56) Mac=SHA1

DES-CBC-SHA Kx=RSA Au=RSA Enc=DES-CBC(56) Mac=SHA1

Riziko

Použití slabých šifrovacích algoritmů snižuje bezpečnost celého šifrovaného spojení.

Doporučení

Doporučujeme daný server nakonfigurovat tak, aby tyto středně slabé šifry nepodporoval. Konkrétní konfigurace se odvíjí od konkrétního serveru (apache, postfix, ...).

3.1.17 Únik informací z hlaviček webového serveru ■

Závažnost: Ovlivněné systémy:

- IP - num_port/tcp.udp
- IP - num_port/tcp.udp
- IP - num_port/tcp.udp

Nález

Během penetračního testu bylo zjištěno, že webový server odesílá ve svých hlavičkách informace o použité verzi jazyka PHP.

[...snip...]

Riziko

Rizikem takového počínání je, že případný útočník má k dispozici informaci o verzi použitého software, který je na serveru nasazen. Tato informace mu může posloužit například ke zjednodušení hledání zranitelností a zpřesnění dalších útoků.

Doporučení

Doporučujeme ve webovém serveru zakázat odesílání těchto potenciálně citlivých informací. Lze toho dosáhnout například přidáním následujících řádků do konfiguračního souboru.

Pro server Apache je to následující nastavení:

```
ServerTokens ProductOnly
ServerSignature Off
```