Virtual Patching pomocí WAF

Virtual Patching pomocí WAF (Web Application Firewall) je proces implementace bezpečnostní politiky, která zabraňuje zneužití známé zranitelnosti na aplikační vrstvě. Zatímco klasický patch opravuje chybu přímo v kódu aplikace, virtuální patch vytvoří ochranné pravidlo na firewallu, který stojí před aplikací.

1. Mechanika ochrany

WAF funguje jako reverzní proxy a zkoumá každý příchozí požadavek (HTTP request). Při virtuálním záplatování se do konfigurační sady WAF přidají specifické instrukce:

- **Signatury:** Detekce konkrétních řetězců nebo vzorců typických pro daný exploit (např. specifické SQL sekvence).
- **Analýza protokolů:** Kontrola, zda požadavek splňuje standardy a neobsahuje neobvyklé anomálie v hlavičkách.
- **Vstupní validace:** Striktní omezení povolených znaků a formátů pro pole, o kterých je známo, že jsou zranitelná.

—

2. Životní cyklus virtuální záplaty

Proces nasazení virtuálního patche pomocí WAF obvykle probíhá v těchto krocích:

```
1. **Detekce:** Organizace obdrží informaci o nové zranitelnosti (např. hlášení CVE).
2. **Verifikace:** Pomocí skeneru zranitelností se potvrdí, že interní aplikace je skutečně ohrožena.
3. **Tvorba pravidla:** Bezpečnostní tým vyvine pravidlo pro WAF (např. v jazyce ModSecurity nebo pomocí rozhraní cloudového poskytovatele).
4. **Testování (Staging):** Pravidlo se nasadí v režimu "Log Only", aby se ověřilo, že neblokuje legitimní uživatele (prevence False Positives).
5. **Vynucení (Enforcement):** Pravidlo se přepne do režimu "Block".
```

—

3. Hlavní výhody tohoto přístupu

- **Okamžitá ochrana:** Vytvoření pravidla pro WAF trvá minuty až hodiny, zatímco vývoj a testování kódu aplikace může trvat týdny.
- **Ochrana neudržovaného SW:** Pro starší aplikace, kde už není k dispozici vývojový tým, je WAF často jedinou cestou, jak splnit požadavky na bezpečnost (compliance).
- **Centralizace:** Jeden virtuální patch na WAF může ochránit celou farmu webových serverů

současně.

—

4. Příklady použití v praxi

Ochrana proti Log4j (Log4Shell)

Když byla v prosinci 2021 objevena kritická chyba v knihovně Log4j, trvalo týdny, než firmy zaktualizovaly všechny své systémy. Poskytovatelé WAF nasadili virtuální patche během hodin, čímž zablokovali řetězce jako `${jndi:ldap://...}` a zachránili tisíce serverů před kompromitací.

Ochrana proti SQL Injection

Pokud je v aplikaci nalezena zranitelnost v přihlašovacím formuláři, WAF může okamžitě začít blokovat klíčová slova jako `UNION SELECT` nebo `OR 1=1` v daném poli, dokud vývojáři nenasadí opravu využívající parametrizované dotazy.

—

5. Omezení a rizika

- **Obcházení (Evasion):** Sofistikovaní útočníci mohou zkoušet různé kódování znaků (např. Hex, Base64), aby pravidlo na WAF obešli.
- **Falešná pozitiva:** Příliš agresivní patch může zablokovat standardní nákupní proces zákazníka.
- **Výkon:** Extrémně velké sady pravidel mohou mírně zvýšit latenci odpovědi serveru.

Související články:

- Obecný princip Virtual Patching
- WAF a síťová bezpečnost
- Penetrační testování a analýza rizik

Tagy: security waf virtual-patching exploits cve vulnerability logging