Cisco Secure Access Warn Action Override-gedrag met IPS-blokinstellingen

Inhoud

uitgeven

Bij het testen van Waarschuwingsgedrag in een toegangsbeleid (Internettoegang) op Cisco Secure Access met IPS ingeschakeld, ervaren gebruikers onverwacht gedrag waarbij de Waarschuwingsactie de IPS-blokkeringsinstellingen lijkt te overschrijven. Bij het openen van een URL die bedoeld is om een IPS-handtekening te activeren (SERVER-WEBAPP /etc/passwd file access attempt, GID-SID: 1-1122), wordt een waarschuwingspagina weergegeven en na bevestiging door de gebruiker is toegang tot de URL toegestaan, ondanks dat IPS is geconfigureerd om het verkeer te blokkeren.

De configuratie omvat:

- Actie: Isoleren
- Inbraakpreventie (IPS): inschakelen
- IPS/blok
- Handtekening: SERVER-WEBAPP /etc/passwd bestandstoegangspoging
- GID-SID: 1-1122

Logboeken voor het zoeken naar activiteiten tonen tegenstrijdige items:

- IPS: (IPS: blok)
- WEB: (WEB: toestaan - waarschuwingspagina weergegeven)
- WEB: (WEB: toestaan - na waarschuwing toegang)

milieu

- Cisco Secure Internet Access Advantage
- Technologie: veilige toegang
- Toegangsbeleid geconfigureerd met actie voor internettoegang en waarschuwing
- IPS ingeschakeld met blokactie voor specifieke handtekeningen

resolutie

Dit gedrag is geïdentificeerd als een defect in Cisco Secure Access, waarbij de actie Waarschuwing in het toegangsbeleid voorrang heeft op de blokkeringsinstellingen van IPS. Het probleem heeft invloed op de interactie tussen de waarschuwingsacties voor toegangsbeleid en de IPS-blokkeringsfunctionaliteit.

Verificatiestappen

Om dit gedrag in uw omgeving te controleren:

Stap 1: toegangsbeleid configureren met waarschuwingsactie en IPS-blokkering inschakelen

- Actie instellen op isoleren met waarschuwingsgedrag
- Inbraakpreventie (IPS) inschakelen
- IPS configureren met blokactie
- Specifieke handtekening toepassen (bijvoorbeeld SERVER-WEBAPP /etc/passwd bestandstoegangspoging, GID-SID: 1-1122)

Stap 2: Test de configuratie door toegang te krijgen tot een URL die de IPS-handtekening activeert

```
https://example.com/etc/passwd
```

Stap 3: Observeer het gedrag

- De waarschuwingspagina wordt weergegeven voor de gebruiker

- Gebruiker kan verder gaan na bevestiging van de waarschuwing
- Toegang tot de URL is toegestaan ondanks de configuratie van het IPS-blok

Stap 4: Controleer de logboeken voor het zoeken naar activiteiten

- Controleer de aanwezigheid van zowel IPS-blok- als WEB allow-vermeldingen
- Bevestig dat de conflicterende logboekvermeldingen het defect aangeven

Huidige status

Dit gedrag is bevestigd als een defect waarbij Warn-actie de IPS-blokinstellingen opheft door het ontwerp in de huidige implementatie. Hetzelfde gedrag treedt op met andere IPS-handtekeningen dan GID-SID: 1-1122, wat aangeeft dat dit een systeemprobleem is dat van invloed is op alle IPS-handtekeningen wanneer Warn-acties worden geconfigureerd.

Een correctieplan en tijdlijn voor dit defect zijn nog niet vastgesteld. Organisaties die dit probleem ondervinden, moeten hun beveiligingsbeleid evalueren en alternatieve configuraties overwegen als strikte IPS-blokkering vereist is.

Oorzaak

De hoofdoorzaak is een defect in Cisco Secure Access, waarbij de verwerking van de actiewaarschuwing voor toegangsbeleid voorrang heeft op de handhaving van IPS-blokkades. Deze ontwerpfout stelt gebruikers in staat om IPS-beveiligingscontroles te omzeilen via het waarschuwingsbevestigingsmechanisme, waardoor de IPS-blokfunctionaliteit effectief wordt vernietigd wanneer waarschuwingsacties worden geconfigureerd.

Cisco Bug ID CSCwt39270 is geassocieerd met deze zaak, hoewel de specifieke relatie tussen deze bug en het waargenomen Warn versus IPS-gedrag nader onderzoek vereist.

Verwante inhoud

- Cisco Technical Support en downloads

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.