Comportamento di override dell'azione di avviso Cisco Secure Access con impostazioni di blocco IPS

Sommario

Problema

Quando si verifica il comportamento Warn in un criterio di accesso (Accesso Internet) su Cisco Secure Access con IPS abilitato, si verifica un comportamento imprevisto quando l'azione Warn sembra ignorare le impostazioni del blocco IPS. In particolare, quando si accede a un URL per attivare una firma IPS (SERVER-WEBAPP /etc/passwd file access try, GID-SID: 1-1122), viene visualizzata una pagina di avviso e, dopo la conferma dell'utente, l'accesso all'URL è consentito anche se l'IPS è stato configurato per bloccare il traffico.

La configurazione include:

- Azione: Isolare
- Prevenzione delle intrusioni (IPS): Abilita
- IPS/Blocco
- Firma: SERVER-WEBAPP /etc/passwd tentativo di accesso ai file
- GID-SID: 1-1122

Nei log di Ricerca attività sono visualizzate voci in conflitto:

- IPS: (IPS: blocco)
- WEB: (WEB: consenti - pagina di avviso visualizzata)
- WEB: (WEB: consenti - dopo l'avviso (accesso)

Ambiente

- Prodotto: Vantaggio Cisco Secure Internet Access
- Tecnologia: Accesso sicuro
- Criterio di accesso configurato con l'azione Accesso a Internet e Avvisa
- IPS abilitato con azione di blocco per firme specifiche

Risoluzione

Questo comportamento è stato identificato come un difetto in Cisco Secure Access, dove l'azione Avvisa nei criteri di accesso ha la precedenza sulle impostazioni dei blocchi IPS. Il problema influisce sull'interazione tra le azioni Avviso criteri di accesso e la funzionalità di blocco IPS.

Fasi di verifica

Per verificare questo comportamento nell'ambiente in uso:

Passaggio 1: Configura i criteri di accesso con l'azione Avvisa e abilita il blocco IPS

- Imposta azione su Isola con comportamento di avviso
- Abilitare la prevenzione delle intrusioni (IPS)
- Configura IPS con azione Blocca
- Applica firma specifica (ad esempio, SERVER-WEBAPP /etc/passwd tentativo di accesso al file, GID-SID: 1-1122)

Passaggio 2: Verificare la configurazione accedendo a un URL che attiva la firma IPS

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

Passaggio 3: Osservare il comportamento

- La pagina di avviso verrà visualizzata all'utente
- L'utente può procedere dopo la conferma dell'avviso
- L'accesso all'URL sarà consentito nonostante la configurazione del blocco IPS

Passaggio 4: Verifica log di ricerca attività

- Verificare la presenza di voci sia di blocco IPS che di voci Web consentite
- Confermare le voci in conflitto nel log per indicare il difetto

Stato corrente

Questo comportamento è stato confermato come un difetto in cui l'azione Avvisa ignora le impostazioni di blocco IPS per progettazione nell'implementazione corrente. Lo stesso comportamento si verifica per le firme IPS diverse da GID-SID: 1-1122, che indica che si tratta di un problema sistemico che interessa tutte le firme IPS quando vengono configurate le azioni di avviso.

Non sono ancora stati definiti il piano di correzione e la tempistica per questo difetto. Le organizzazioni che riscontrano questo problema devono valutare i propri criteri di sicurezza e prendere in considerazione configurazioni alternative se è necessario un rigoroso blocco IPS.

Causa

La causa principale è un difetto di Cisco Secure Access in cui l'elaborazione dell'azione Avviso dei criteri di accesso ha la precedenza sull'imposizione dei blocchi IPS. Questo difetto di progettazione consente agli utenti di ignorare i controlli di sicurezza IPS tramite il meccanismo di conferma dell'avviso, annullando in modo efficace la funzionalità di blocco IPS quando vengono configurate le azioni di avviso.

A questo caso è associato l'ID bug Cisco CSCwt39270, ma la relazione specifica tra questo bug e il comportamento Warn vs IPS osservato richiede un'ulteriore analisi.

Contenuto correlato

- Supporto tecnico Cisco e download

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).