Risolvere i problemi relativi alle intrusioni in FMC con Impact=Unknown

Sommario

Problema

Dopo la distribuzione di un nuovo centro di gestione dei firewall e l'aggiornamento alla versione 7.7.12, tutti gli eventi di intrusione visualizzano "Impact=Unknown" anziché i valori di impatto previsti. In questo modo si evita l'attivazione di meccanismi di avviso appropriati, poiché il campo dell'impatto è necessario per la configurazione degli avvisi.

Ambiente

- FMC versione 7.7.12. Possono essere interessate anche altre versioni software.
- Criteri intrusione in modalità Prevenzione o Rilevamento.

Risoluzione

Per risolvere questo problema, è necessario verificare e configurare l'ambito dei criteri di individuazione in modo da includere tutti gli indirizzi IP rilevanti in cui vengono generati eventi di intrusione.

Passaggio 1. Identificazione degli indirizzi IP interessati

Esaminare gli eventi di intrusione che mostrano "Impact=Unknown" e identificare gli indirizzi IP specifici coinvolti in questi eventi. Documentare questi indirizzi IP per il confronto con la

configurazione corrente dei criteri di individuazione.

Passaggio 2. Verifica della configurazione corrente dei criteri di individuazione

Passare a Criteri FMC > Individuazione rete (nelle versioni più recenti è Criteri > Avanzate > Individuazione rete) ed esaminare le impostazioni correnti dei criteri di individuazione per determinare quali intervalli di indirizzi IP o subnet sono attualmente inclusi nell'ambito di individuazione.

Passaggio 3. Aggiornamento dell'ambito dei criteri di individuazione

Modificare la configurazione dei criteri di individuazione per includere tutti gli indirizzi IP in cui si verificano eventi di intrusione. Verificare che l'ambito dei criteri di individuazione comprenda tutti i segmenti di rete in cui si prevede di ricevere eventi di intrusione con una corretta valutazione di impatto.

Passaggio 4. Distribuire le modifiche alla configurazione

Distribuire la configurazione aggiornata dei criteri di individuazione su tutti i dispositivi gestiti per garantire che le modifiche abbiano effetto sull'intera infrastruttura di sicurezza.

Passaggio 5. Verifica popolamento campo impatto

Monitorare i nuovi eventi di intrusione per verificare che nel campo di impatto siano stati inseriti valori appropriati anziché "Sconosciuto".

Causa

Gli eventi di intrusione con "Impact=Unknown" sono stati causati da un problema di configurazione in cui gli indirizzi IP interessati non sono stati inclusi in alcun criterio di individuazione nel FMC. Quando gli indirizzi IP non rientrano nell'ambito dei criteri di individuazione configurati, il FMC non è in grado di valutare correttamente l'impatto degli eventi di intrusione per tali indirizzi, pertanto nel campo dell'impatto vengono inseriti valori "Sconosciuti". Si tratta di un problema relativo alla configurazione piuttosto che un problema software o hardware.

Contenuto correlato

- Livelli di impatto degli eventi di intrusione
- 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).