Cisco Secure Access Warnaktion setzt Verhalten durch IPS-Blockierungseinstellungen außer Kraft

Inhalt

Problem

Beim Testen des Warnverhaltens in einer Zugriffsrichtlinie (Internetzugriff) für Cisco Secure Access mit aktiviertem IPS zeigen Benutzer ein unerwartetes Verhalten, bei dem die Warnaktion die IPS-Blockeinstellungen außer Kraft zu setzen scheint. Insbesondere beim Zugriff auf eine URL, die eine IPS-Signatur auslösen soll (SERVER-WEBAPP /etc/passwd file access attempts, GID-SID: 1-1122) wird eine Warnseite angezeigt. Nach der Bestätigung durch den Benutzer wird der Zugriff auf die URL zugelassen, obwohl IPS so konfiguriert ist, dass der Datenverkehr blockiert wird.

Die Konfiguration umfasst:

- Aktion: Isolieren
- Intrusion Prevention (IPS): Enable
- IPS/Baustein
- Unterschrift: SERVER-WEBAPP /etc/passwd-Dateizugriffsversuch
- GID-SID: 1-1122

Aktivitätssuchprotokolle zeigen in Konflikt stehende Einträge an:

- IPS: (IPS: blockieren)
- WEB: (WEB: allow - angezeigte Warnseite)
- WEB: (WEB: allow - Zugriff nach Warnung)

Umwelt

- Produkt: Cisco Secure Internet Access - Vorteile
- Technologie: Sicherer Zugriff
- Mit Internetzugriff und Warnaktionen konfigurierte Zugriffsrichtlinie
- IPS mit Blockierungsaktion für bestimmte Signaturen aktiviert

Auflösung

Dieses Verhalten wurde in Cisco Secure Access als Defekt identifiziert, bei dem die Warnaktion in den Zugriffsrichtlinien Vorrang vor den IPS-Blockeinstellungen hat. Das Problem wirkt sich auf die Interaktion zwischen Warnaktionen für die Zugriffsrichtlinie und der IPS-Sperrfunktion aus.

Verifizierungsschritte

So überprüfen Sie dieses Verhalten in Ihrer Umgebung:

Schritt 1: Konfigurieren der Zugriffsrichtlinie mit Warnaktion und Aktivieren der IPS-Blockierung

- Aktion für Isolierung mit Warnverhalten festlegen
- Aktivieren von Intrusion Prevention (IPS)
- IPS mit Blockierungsaktion konfigurieren
- Anwenden einer bestimmten Signatur (z. B. SERVER-WEBAPP /etc/passwd file access attempts, GID-SID: 1-1122)

Phase 2: Testen der Konfiguration durch Zugriff auf eine URL, die die IPS-Signatur auslöst

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

Schritt 3: Verhalten beobachten

- Dem Benutzer wird eine Warnseite angezeigt.
- Der Benutzer kann fortfahren, nachdem er die Warnung bestätigt hat.

- Der Zugriff auf die URL ist trotz der Konfiguration der IPS-Sperre zulässig.

Schritt 4: Aktivitätssuchprotokolle überprüfen

- Überprüfen des Vorhandenseins von IPS-Block- und WEB-Zulassungseinträgen
- Bestätigen Sie die widersprüchlichen Protokolleinträge, um den Fehler anzuzeigen.

Aktueller Status

Dieses Verhalten wurde als Fehler bestätigt, bei dem die Warnaktion die IPS-Blockeinstellungen in der aktuellen Implementierung per Design überschreibt. Dasselbe Verhalten tritt bei anderen IPS-Signaturen als GID-SID auf: 1-1122 ein, das darauf hinweist, dass es sich bei der Konfiguration von Warnaktionen um ein systemisches Problem handelt, das alle IPS-Signaturen betrifft.

Ein Korrekturplan und ein Zeitplan für diesen Mangel sind noch nicht festgelegt. Unternehmen mit diesem Problem sollten ihre Sicherheitsrichtlinien auswerten und alternative Konfigurationen in Betracht ziehen, wenn eine strikte IPS-Blockierung erforderlich ist.

Ursache

Die Ursache liegt in einem Fehler in Cisco Secure Access, bei dem die Verarbeitung der Zugriffsrichtlinien-Warnaktion Vorrang vor der IPS-Blockdurchsetzung hat. Dieser Designfehler ermöglicht es Benutzern, die IPS-Sicherheitskontrollen mithilfe des Warnbestätigungsmechanismus zu umgehen und macht die IPS-Blockfunktion praktisch ungültig, wenn Warnaktionen konfiguriert werden.

Cisco Bug-ID CSCwt39270 ist mit diesem Fall verbunden, obwohl die spezifische Beziehung zwischen diesem Fehler und dem beobachteten Warn/IPS-Verhalten einer weiteren Untersuchung bedarf.

Verwandte Inhalte

- Technischer Support und Downloads von Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.