Secure Access Warn Action Override Behavior with IPS Block Settings

Contents

Issue

When testing Warn behavior in an Access Policy (Internet Access) on Cisco Secure Access with IPS enabled, users experience unexpected behavior where the Warn action appears to override IPS block settings. Specifically, when accessing a URL intended to trigger an IPS signature (SERVER-WEBAPP /etc/passwd file access attempt, GID-SID: 1-1122), a warning page is displayed and after user confirmation, access to the URL is allowed despite IPS being configured to block the traffic.

The configuration includes:

- Action: Isolate
- Intrusion Prevention (IPS): Enable
- IPS / Block
- Signature: SERVER-WEBAPP /etc/passwd file access attempt
- GID-SID: 1-1122

Activity Search logs show conflicting entries:

- IPS: (IPS: block)
- WEB: (WEB: allow - warning page displayed)
- WEB: (WEB: allow - after warning access)

Environment

- Product: Cisco Secure Internet Access Advantage
- Technology: Secure Access

- Access Policy configured with Internet Access and Warn action
- IPS enabled with block action for specific signatures

Resolution

This behavior has been identified as a defect in Cisco Secure Access where the Warn action in Access Policies takes precedence over IPS block settings. The issue affects the interaction between Access Policy Warn actions and IPS blocking functionality.

Verification Steps

To verify this behavior in your environment:

Step 1: Configure Access Policy with **Warn** action and enable IPS blocking:

- Set **Action to Isolat**e with **Warn** behavior.
- Enable **Intrusion Prevention (IPS**).
- Configure **IPS with Block action**.
- Apply specific signature (such as SERVER-WEBAPP /etc/passwd file access attempt, GID-SID: 1-1122).

Step 2: Test the configuration by accessing a URL that triggers the IPS signature:

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

Step 3: Observe the behavior:

- Warning page is displayed to the user.
- User can proceed after confirming the warning.
- Access to the URL is allowed despite IPS block configuration.

Step 4: Check Activity Search logs:

- Verify presence of both IPS block and WEB allow entries.
- Confirm the conflicting log entries indicate the defect.

Current Status

This behavior has been confirmed as a defect where Warn action overrides IPS block settings by design in the current implementation. The same behavior occurs with IPS signatures other than GID-SID: 1-1122, indicating this is a systemic issue affecting all IPS signatures when Warn actions are configured.

A correction plan and timeline for this defect have not yet been determined. Organizations experiencing this issue ought to evaluate their security policies and consider alternative configurations if strict IPS blocking is required.

Cause

The root cause is a defect in Cisco Secure Access where the Access Policy Warn action processing takes precedence over IPS block enforcement. This design flaw allows users to bypass IPS security controls through the warning confirmation mechanism, effectively nullifying the IPS block functionality when Warn actions are configured.

Related Content

- Cisco Technical Support & Downloads