Snort Engine Upgrade Blocked During FTD Upgrade Due to Custom Policy Detection

Contents

Issue

During an FTD upgrade from version 7.2 to 7.4.4 on an HA FPR-4115 managed by FMC, the Snort engine upgrade to Snort 3 is blocked with error messages indicating failure to convert Snort 2 custom rules or use of custom intrusion or network analysis policies. The specific error message states: "Cannot upgrade to Snort 3. Device uses at least one custom intrusion policy or network analysis policy." A more detailed failure message references inability to convert Snort 2 custom rules and points to /var/sf/htdocs/ips/snort.rej for details. The concern is whether this error would prevent migration to Snort 3 and impact inspection functionality.

Environment

- Cisco Secure Firewall Firepower version 7.3
- Firepower Management Center (FMC) version 7.7.11
- FTD devices in High Availability (HA) configuration
- Hardware: FPR-4115
- Upgrade path: FTD 7.2 to 7.4.4
- VDB at latest version prior to upgrade
- Local Rules section under Objects > Intrusion Rules > Snort 2 All Rules is empty

Resolution

The error message blocking the Snort engine upgrade is documented behavior related to Cisco bug ID CSCwn46794

Verification Steps

Step 1: Verify Custom Snort 2 Rules Status

Navigate to the FMC interface and check for custom Snort 2 rules:

```
Objects > Intrusion Rules > Snort 2 All Rules > Local Rules
```

Step 2: Confirm VDB Version

Ensure that the Vulnerability Database (VDB) is at the latest version before proceeding with the upgrade.

Step 3: Review Error Details

Check the detailed error information in the referenced file:

```
/var/sf/htdocs/ips/snort.rej
```

Upgrade Process

When the "Local Rules" section is confirmed to be empty (no custom Snort 2 rules present), the upgrade can proceed

Step 1: Proceed with Snort 3 Upgrade

Continue with the FTD upgrade process to version 7.4.4, which includes the Snort 3 engine upgrade.

Step 2: Post-Upgrade Validation

After the upgrade completes successfully, test traffic flow to confirm expected behavior with Snort 3 engine.

Step 3: Monitor System Performance

Validate that inspection functionality operates as expected with the new Snort 3 engine.

Cause

The upgrade blocking message is documented behavior associated with Cisco bug ID CSCwn46794. This bug cause
upgrade validation incorrectly identifies the presence of custom policies.

Related Content

- Cisco bug ID CSCwn46794
- Cisco bug ID CSCwk07199
- Cisco Technical Support & Downloads