

Secure Access DLP-bestandsgrootteregels zonder gegevensclassificatie genereren geen monitorgebeurtenissen voor tekstbestanden

Inhoud

uitgifte

Een Cisco Secure Access Web DLP-beleid dat alleen is geconfigureerd met criteria voor bestandsgrootte (geen gegevensclassificatie) genereert geen DLP-monitorgebeurtenissen voor het uploaden van .txt-bestanden, terwijl hetzelfde beleid correct monitorgebeurtenissen activeert voor andere bestandstypen zoals .xlsx-, .png- en .pdf-bestanden. Het getroffen beleid Senior Management Policy - Web is geconfigureerd met:

- Bestandsbeheer met aangepaste bestandsgrootte tussen 1 KB en 49 MB
- Geen criteria voor gegevensclassificatie
- Actie ingesteld op Monitor

Uit de tests bleek dat:

- Het uploaden van TXT-bestanden wordt niet weergegeven in DLP-gebeurtenissen wanneer Actie = Monitor.
- Dezelfde TXT-bestanden genereren DLP-gebeurtenissen correct wanneer Action = Block.
- Activiteitenlogboeken tonen alle bestanden die worden geüpload, inclusief TXT-bestanden.
- Andere bestandsformaten (PNG, PDF, XLSX) genereren DLP-gebeurtenissen zoals verwacht met Monitor-actie.

Bovendien, wanneer er geen gegevensclassificatie is geconfigureerd in DLP-regels, tonen de geregistreerde DLP-gebeurtenissen altijd een gemiddelde ernst, ongeacht de ingestelde regelernst.

milieu

- Cisco Secure Access (voorheen Cisco Umbrella)
- DLP (Data Loss Prevention)-webbeleid
- Internettoegangsbeleid met HTTPS-decodering ingeschakeld
- Testen van uploaden van bestanden via webtoepassingen

resolutie

Dit gedrag is ongedocumenteerd, maar wordt verwacht door het ontwerp. MIME-typen zoals tekst/onbewerkte tekst worden overgeslagen van DLP-bewaking wanneer alleen criteria voor bestandsgrootte worden gebruikt met Monitor-actie om overbelasting van logbestanden te voorkomen. Het ontwikkelteam bevestigde dat dit opzettelijk gedrag is dat niet extern is gedocumenteerd.

Opties voor tijdelijke oplossing

Optie 1 (aanbevolen): gegevensclassificatie toevoegen

Voeg eventuele brede criteria voor gegevensclassificatie toe aan de DLP-regel en houd Actie = Monitor.

Dit herstelt:

- Gebeurtenisgeneratie TXT-bestand DLP
- Correcte verwerking van de ernst op basis van de regelconfiguratie

Optie 2: Actie wijzigen om te blokkeren

Wijzig de regelactie van Monitor in Block. Dit genereert DLP-gebeurtenissen voor TXT-bestanden, maar dwingt ook blokkering af die niet kan worden gewenst voor alleen-bewakingsgevallen.

Resultaten laboratoriumtests

Uitgebreide laboratoriumtests bevestigden de gedragspatronen.

Testscenario 1: DLP-regel met gegevensclassificatie en bestandsgrootte (1 KB-49 MB), actie = blok

- TXT-bestand met PII: geblokkeerd en geregistreerd
- PDF-bestand: geblokkeerd en vastgelegd
- TXT-bestand zonder PII: Toegestaan (verwacht)
- PNG met PII: toegestaan (verwacht op basis van classificatie)

Testscenario 2: DLP-regel met alleen bestandsgrootte (geen gegevensclassificatie), actie = blok

- Alle bestandstypen (TXT, PDF, PNG): geblokkeerd en vastgelegd
- De ernst wordt weergegeven als Medium, ondanks de regel die is geconfigureerd als Laag

Testscenario 3: DLP-regel met alleen bestandsgrootte (geen gegevensclassificatie), actie = monitor

- TXT-bestanden: toegestaan, maar NIET aangemeld bij DLP-gebeurtenissen
- PDF- en PNG-bestanden: toegestaan en aangemeld bij DLP-gebeurtenissen
- Activiteitenlogboeken tonen alle uploads inclusief TXT-bestanden

Oorzaak

Dit is opzettelijk maar ongedocumenteerd gedrag in Cisco Secure Access DLP. Het systeem omzeilt de logboekregistratie van DLP-gebeurtenissen voor tekst-/gewone MIME-typen bij het gebruik van regels voor alleen bestandsgrootte met Monitor-actie om overmatige loggeneratie te voorkomen. Het gedrag is actie-afhankelijk en MIME-type specifiek:

- Actie bewaken met alleen criteria voor bestandsgrootte: TXT-bestanden die uit de logboekregistratie zijn overgeslagen
- Actie blokkeren met alleen criteria voor bestandsgrootte: TXT-bestanden die normaal zijn gelogd
- Elke actie met aanwezige gegevensclassificatie: TXT-bestanden die normaal zijn gelogd

Het probleem met de ernst treedt op omdat DLP-gebeurtenissen ernst afleiden van metagegevens voor gegevensclassificatie in plaats van regelinstellingen bij het werken in de inhoudsbewuste modus. Zonder gegevensclassificatie wordt het systeem standaard ingesteld op de "Medium"-ernst, ongeacht de geconfigureerde regelnst.

Gerelateerde inhoud

- [Configuratie van bestandsgrootte Cisco Secure Access DLP](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.