Microsoft

"When confidential data looks Ordinary: Metadata Gaps driving Cross-Tenant Breaches"

VULN-162338

Report created.
Sep 4, 2025, 10:22 PM

Description

This vulnerability arises when sensitive unstructured data files (classified as Confidential or Strictly Confidential) are not embedded with classification or sensitivity labels in their metadata. In the absence of classification, files become indistinguishable from ordinary non-sensitive data. Security technologies such as Data Loss Prevention (DLP), Endpoint Detection & Response (EDR), Extended Detection & Response (XDR), and Network Detection & Response (NDR) depend heavily on metadata-driven classification to apply stricter inspection, routing, and enforcement policies.

Without classification metadata, sensitive files may bypass automated safeguards and remain unprotected at rest, in transit, or during processing. Attackers, malicious insiders, or even inadvertent user actions can exploit this weakness to exfiltrate, misroute, or mishandle sensitive information through seemingly benign activities such as renaming, format conversion, steganography, zipping with encryption, cloud uploads, or embedding into collaborative tools like Teams or Slack. Since no metadata flags are present, these activities appear normal to security controls.

This vulnerability has significant implications in multi-tenant or outsourcing environments:

Breakdown of Logical Segregation: Unclassified files from one tenant may be processed, backed up, or encrypted with the same keys as files from another tenant. This collapses logical and cryptographic boundaries, creating unintended cross-tenant exposure.

Loss of Encryption Integrity: Classification often dictates encryption key assignment. Without it, files may default to shared keys, meaning that compromise of one tenant's environment can indirectly expose another tenant's data.

Type a new message

Status