Status of Proofpoint Products with CVE-2021-44228

Dec 14, 2021 · News Channels

DESCRIPTION

A critical remote code execution vulnerability affecting the popular Java logging package log4j2, CVE-2021-44228, was published on December 10, 2021. The vulnerability is also referred to as Log4Shell. The following table indicates whether the vulnerability applies to specific Proofpoint products. For information relating to our ongoing investigation into Log4Shell, see this article.

Product	Status
Archiving Appliance	Impacted, remediation in progress. Please contact support to schedule your update
Archiving Backend	Impacted, remediation implemented
Cloud App Security Broker	Impacted, remediation in progress
Cloudmark on Premise	Not Impacted
Cloudmark Cloud/Cloudmark Hybrid	Impacted, remediation implemented
DLP Core Engine	Not Impacted
Email Continuity	Impacted, remediation implemented
Essentials Archive	Impacted, remediation implemented
Essentials Email	Not Impacted
Email Fraud Defense (EFD)	Not Impacted
Email Protection on Demand (PoD), including Email DLP and Email Encryption	Impacted, remediation implemented

Product	Status
Email Protection On-Premise (PPS), including Email DLP and Email Encryption	Impacted, remediation implemented. If your deployment is configured to manually apply patches, please reach out to support for help or to verify if the remediation was applied
Endpoint DLP	Not Impacted
Insider Threat Management On-prem	Not Impacted
Insider Threat Management SaaS	Impacted, remediation in progress
Isolation	Not Impacted
Meta/ZTNA	Impacted, remediation in progress
Nexus People Risk Explorer	Not Impacted
Proofpoint Compliance Gateway	Impacted, remediation implemented
Secure Share	Not Impacted
Security Awareness Training	Impacted, remediation implemented
Sentrion 4.5	Impacted, remediation implemented - Please reach out to support for help or to verify if the remediation was applied
Sentrion 4.4 or earlier	Not Impacted
SocialPatrol	Impacted, remediation implemented
SocialWare	Impacted, remediation implemented
Targeted Attack Protection (TAP)	Not Impacted
Threat Response (TRAP)	Not Impacted
Web Security	Impacted, remediation in progress

Impacted, remediation implemented = Proofpoint product used a version of the Log4j software identified as vulnerable in CVE-2020-44228 and Proofpoint has implemented the open source project's recommended mitigation
Impacted, remediation in progress = Proofpoint product uses a version of the Log4j software identified as vulnerable in CVE-2020-44228 and Proofpoint is in the process of implementing the open source project's recommended mitigation
Not Impacted = Proofpoint product does not use a Log4j version vulnerable to CVE-2020-44228

LAST PUBLISHED DATE
12/14/2021 1:21 AM

FILE

ARTICLE NUMBER
000009837