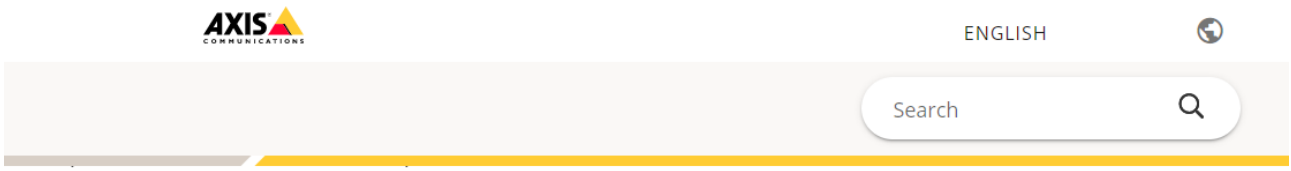
LOG4J VULNERABILITY – Comunicazioni dei Vendor

AXIS COMMUNICATIONS



CVE	Result of investigation | Actions
CVE-2021-44228	Not affected. AXIS OS products only use the vanilla Apache webserver and **not** Apache Log4j, which is vulnerable.

https://help.axis.com/axis-os

AVIGILON

Resolution

Below is the current status of our impact reviews:

Product Line	Status	Next Steps
Avigilon Control Center 6.x and 7.x	Not Impacted	N/A
Avigilon Cloud Services (ACS)	Not Impacted	N/A
Avigilon HD, H3, H4 and H5 cameras	Not Impacted	N/A
Avigilon 4-port encoders	Not Impacted	N/A
Avigilon presence detector	Not Impacted	N/A
Access Control Manager (ACM)	Not Impacted	N/A
ACM Expedite	Not Impacted	N/A
Mercury Hardware	Not Impacted	N/A
HID VertX EVO Hardware	Not Impacted	N/A
Compass	Impacted	Mitigation procedure available by Dec 17th. Hot fix with full resolution available by Dec 31st.
Halo Smart Sensor	Under Review	
IP Horn Speaker	Under Review	

VIVOTEK

Security Advisory

Advisory ID	Advisory	CVE ID	Status	Last Updated
VVTK-SA-2021-01	No VIVOTEK Products are Affected by Apache Log4j Vulnerability	CVE-2021-44228	Confirmed	December 16, 2021

http://download.vivotek.com/downloadfile/support/cyber-security/vvtk-sa-2021-01_v1.pdf

PELCO

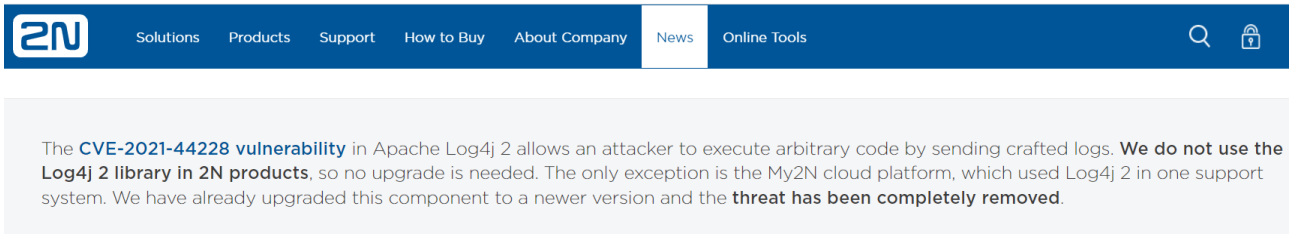
Based on our current analysis, the following Motorola Solutions products are not affected by the Log4J vulnerability:

- VideoXpert
- Endura
- Sarix Enh
- Sarix Pro
- ExSite
- Spectra Enh
- Spectra Pro
- Optera
- Esprit
- Sarix TI

We have determined that the following Motorola Solutions products may be impacted by the Log4J vulnerability:

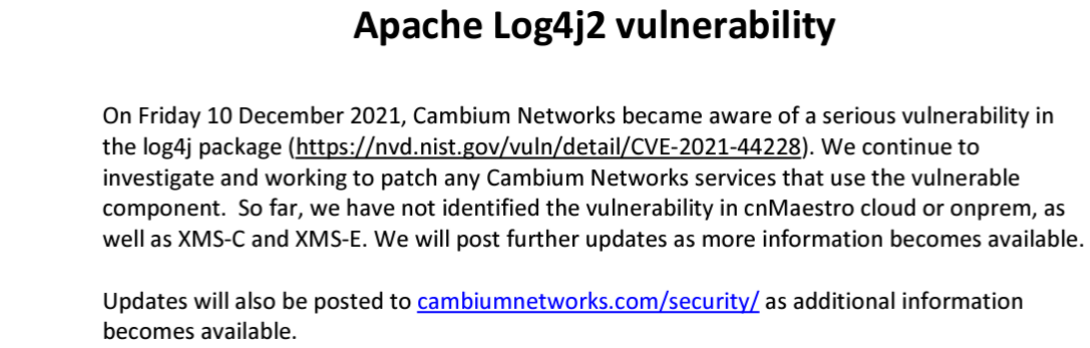
- Compass Decision Management System
  Remediation: Mitigation procedure in progress. Hot fix with full resolution available by December 31, 2021.
- Digital Sentry
  Remediation: Under review.
- Pelco Sarix Value & EVO Cameras and NET5500
  Remediation: Under review.

2N



https://www.2n.com/en_US/news/2n-products-are-not-threatened-by-the-log4j-2-vulnerability-cve-2021-44228

CAMBIUM NETWORKS



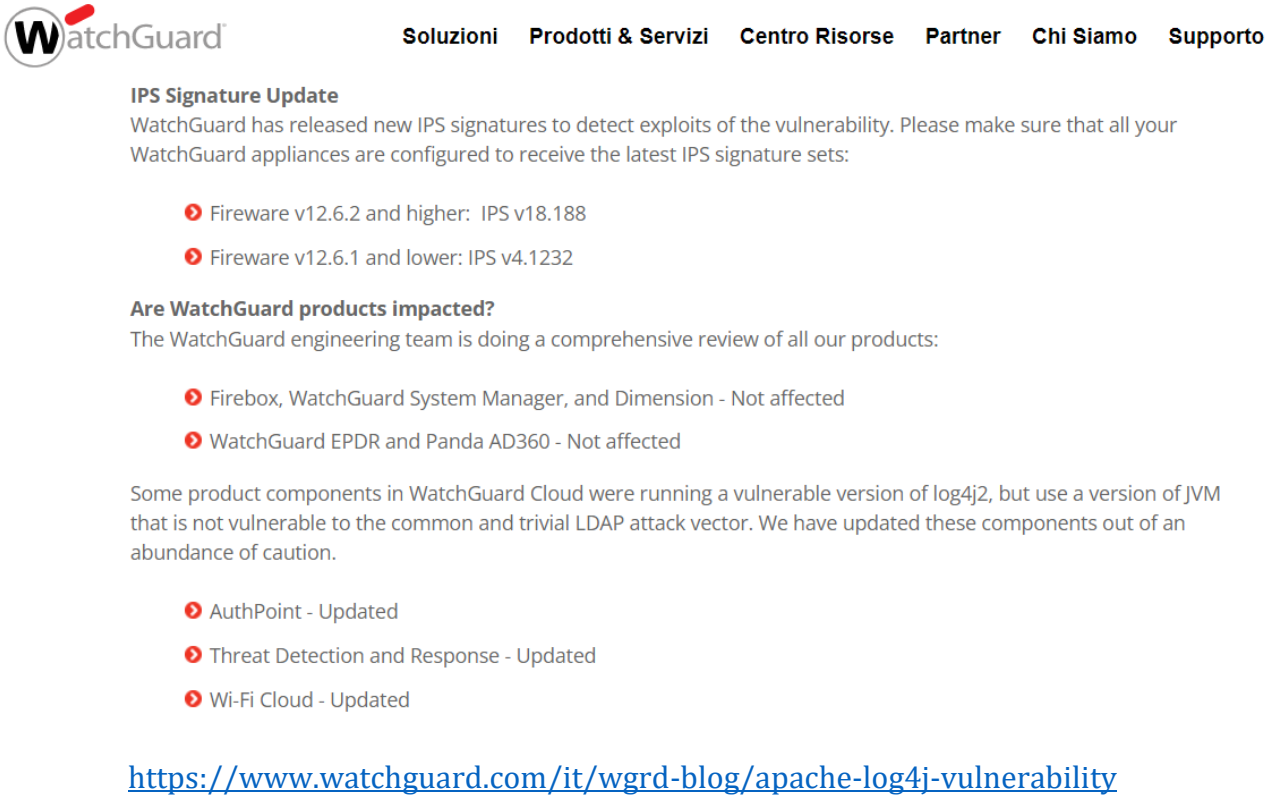
Apache Log4j2 vulnerability

On Friday 10 December 2021, Cambium Networks became aware of a serious vulnerability in the log4j package (https://nvd.nist.gov/vuln/detail/CVE-2021-44228). We continue to investigate and working to patch any Cambium Networks services that use the vulnerable component. So far, we have not identified the vulnerability in cnMaestro cloud or onprem, as well as XMS-C and XMS-E. We will post further updates as more information becomes available.

Updates will also be posted to cambiumnetworks.com/security/ as additional information becomes available.

https://www.cambiumnetworks.com/wp-content/uploads/2021/12/Apache-Log4j2-vulnerability.pdf

WATCHGUARD



WatchGuard Soluzioni Prodotti & Servizi Centro Risorse Partner Chi Siamo Supporto

IPS Signature Update

WatchGuard has released new IPS signatures to detect exploits of the vulnerability. Please make sure that all your WatchGuard appliances are configured to receive the latest IPS signature sets:

- Fireware v12.6.2 and higher: IPS v18.188
- Fireware v12.6.1 and lower: IPS v4.1232

Are WatchGuard products impacted?

The WatchGuard engineering team is doing a comprehensive review of all our products:

- Firebox, WatchGuard System Manager, and Dimension - Not affected
- WatchGuard EPDR and Panda AD360 - Not affected

Some product components in WatchGuard Cloud were running a vulnerable version of log4j2, but use a version of JVM that is not vulnerable to the common and trivial LDAP attack vector. We have updated these components out of an abundance of caution.

- AuthPoint - Updated
- Threat Detection and Response - Updated
- Wi-Fi Cloud - Updated

https://www.watchguard.com/it/wgrd-blog/apache-log4j-vulnerability