White Paper

log4j vulnerability analysis

Directory
Phone Directory
Jabber UDS Server
Web Directory
IPS Popup / Reverse Lookup
Personal Directory
Video Collaboration Endpoints
Webex Directory
ClickNDial
Switchboard/IVR/Group
Attendant Console
Tannounce
Line Group Manager
Silent Monitoring
Admin tools
Morning Check
Phone Remote
Phone Robot
Provisioning
Phone Deployment
Manager Assistant
IP Phone / Jabber Interface

Productivity tools
IPS Phone Config
IPS Lock
Wakeup Call
Missed Call Alerter
Conference Center
Busy Alerter Callback
Desktop Popup for CRM
Finesse Gadgets
Alerting
Voice Alert
IPS Pager
Extension Mobility tools
TSSO
Delog / Relog
Pin & Password Manager
Recording
Call Recording
Recording Notification
Video Collaboration Endpoints
Applications Suite

December 15th, 2021

1 Log4j vulnerability analysis

Following the announcement of Log4j vulnerability, CVE-2021-44228, telisca has carefully analyzed it potential utilization in telisca applications.

The only module written in Java is telisca CTI Server used by several telisca applications.

We have found that log4j library was only included in telisca Setup versions 7.3.1.00x released during August 2021.

However, the version of log4j installed was v1.x which is NOT in the range of the current discovered vulnerability versions (between 2.x and 2.15.0).

It was used by a very specific modules, that checked Extension Mobility duplicated login, was enabled with a specific license and which did not include any user interaction/Web interface.

It was removed since telisca Setup version 7.3.2 (September 9th, 2021). Current of Setup version is 7.4.1.

We have also checked that our setup does not include any affected Java third party software, that may embed log4j.

So there is NO risk with telisca applications.