Stellungnahme

byon vTK System und Log4Shell / log4j

Derzeit gibt es eine massive Sicherheitslücke in der Java-Software-Bibliothek log4j.

Diese ist vom Bundesamt für Sicherheit in der Informationstechnik als extrem kritisch eingestuft worden.

https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2021/2021-549032-10F2.pdf

Für die Plattform der vTK Kommunikationslösung kommen Lösungen unterschiedlicher Anbieter zum Tragen, welche entsprechend geprüft haben. Unsere Partner sind nicht von der Sicherheitslücke betroffen.

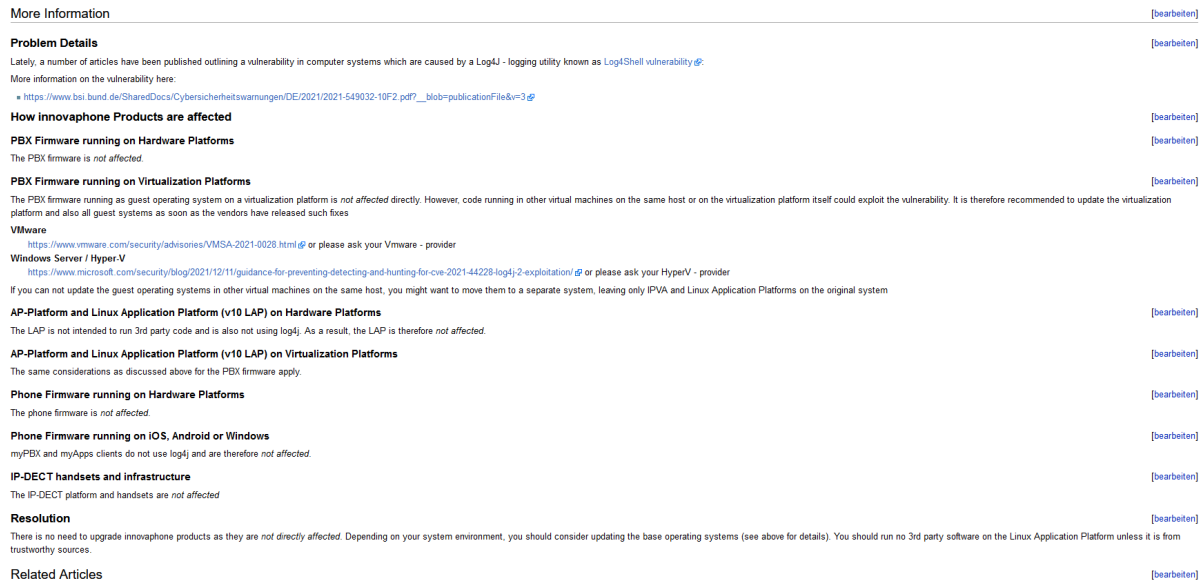
Diese sind:

Innovaphone

Innovaphone ist nicht von der Sicherheitslücke betroffen.

http://wiki.innovaphone.com/index.php?title=Support:Innovaphone_products_not_vulnerable_to_Log4J_exploit (Link kann aber nicht ohne Login aufgerufen werden)

Unten der Screenshot des Links



More Information [bearbeiten]

Problem Details [bearbeiten]

Lately, a number of articles have been published outlining a vulnerability in computer systems which are caused by a Log4J - logging utility known as Log4Shell vulnerability:

More information on the vulnerability here:

- https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2021/2021-549032-10F2.pdf?__blob=publicationFile&v=3

How innovaphone Products are affected [bearbeiten]

PBX Firmware running on Hardware Platforms [bearbeiten]

The PBX firmware is *not affected*.

PBX Firmware running on Virtualization Platforms [bearbeiten]

The PBX firmware running as guest operating system on a virtualization platform is *not affected* directly. However, code running in other virtual machines on the same host or on the virtualization platform itself could exploit the vulnerability. It is therefore recommended to update the virtualization platform and also all guest systems as soon as the vendors have released such fixes

VMware

- https://www.vmware.com/security/advisories/VMSA-2021-0028.html or please ask your Vmware - provider

Windows Server / Hyper-V

- https://www.microsoft.com/security/blog/2021/12/11/guidance-for-preventing-detecting-and-hunting-for-cve-2021-44228-log4j-2-exploitation/ or please ask your HyperV - provider

If you can not update the guest operating systems in other virtual machines on the same host, you might want to move them to a separate system, leaving only IPVA and Linux Application Platforms on the original system

AP-Platform and Linux Application Platform (v10 LAP) on Hardware Platforms [bearbeiten]

The LAP is not intended to run 3rd party code and is also not using log4j. As a result, the LAP is therefore *not affected*.

AP-Platform and Linux Application Platform (v10 LAP) on Virtualization Platforms [bearbeiten]

The same considerations as discussed above for the PBX firmware apply.

Phone Firmware running on Hardware Platforms [bearbeiten]

The phone firmware is *not affected*.

Phone Firmware running on iOS, Android or Windows [bearbeiten]

myPBX and myApps clients do not use log4j and are therefore *not affected*.

IP-DECT handsets and infrastructure [bearbeiten]

The IP-DECT platform and handsets are *not affected*

Resolution [bearbeiten]

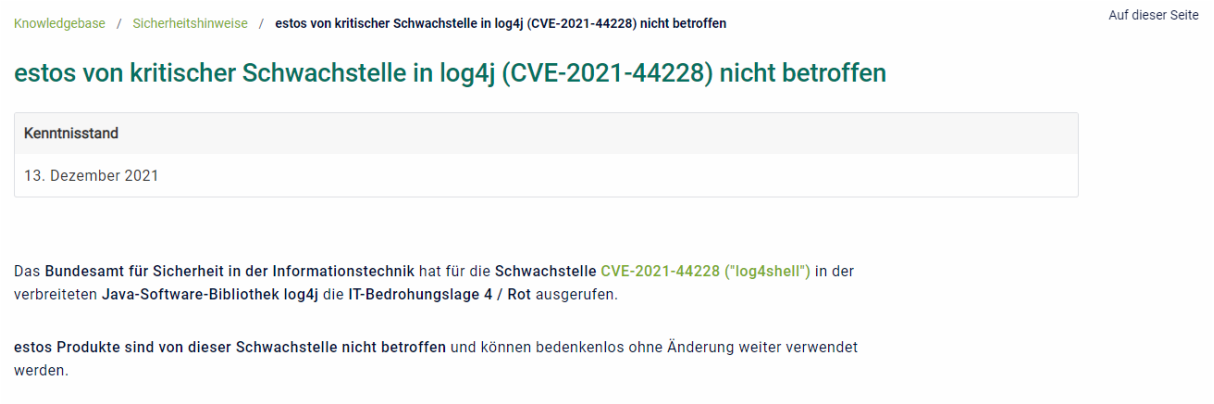
There is no need to upgrade innovaphone products as they are *not directly affected*. Depending on your system environment, you should consider updating the base operating systems (see above for details). You should run no 3rd party software on the Linux Application Platform unless it is from trustworthy sources.

Related Articles [bearbeiten]

Estos

Estos ist nicht von der Sicherheitslücke betroffen.

https://support.estos.de/de/sicherheitshinweise/estos-von-kritischer-schwachstelle-in-log4j-cve-2021-44228-nicht-betroffen



Knowledgebase / Sicherheitshinweise / **estos von kritischer Schwachstelle in log4j (CVE-2021-44228) nicht betroffen**

Auf dieser Seite

estos von kritischer Schwachstelle in log4j (CVE-2021-44228) nicht betroffen

Kenntnisstand
13. Dezember 2021

Das **Bundesamt für Sicherheit in der Informationstechnik** hat für die **Schwachstelle** CVE-2021-44228 ("log4shell") in der verbreiteten **Java-Software-Bibliothek log4j** die **IT-Bedrohungslage 4 / Rot** ausgerufen.

estos Produkte sind von dieser Schwachstelle nicht betroffen und können bedenkenlos ohne Änderung weiter verwendet werden.

Webserver für Portal Zugriff

Die Webanwendungen auf den Webservern sind von uns selbst programmiert. Es wird dort an keiner Stelle die betroffene Bibliothek verwendet.