ondeso | SUCCESS STORY

CVE-2021-44228: LOG4SHELL PATCHING WITH ONDESO SR

A cyber security engineer from the automotive industry was faced with the challenge of closing the critical Log4Shell vulnerability on 2,000 OT clients as quickly as possible. Thanks to our proven ondeso SR software, he found an automated solution to quickly identify and close the vulnerability.

The Log4Shell vulnerability, also known as CVE-2021-44228, posed a serious risk to organizations due to the widespread use of the Apache Log4j software framework in numerous systems and applications. This critical vulnerability allowed attackers to execute arbitrary code and compromise systems, leading to significant security risks. A cyber security engineer responsible for 2,000 OT clients in a manufacturing company in the automotive industry recognized the urgency of the situation. The vulnerability posed a serious threat to ongoing operations and required a rapid response to prevent potential production downtime and security leaks. As ondeso SR has been used worldwide in the group for several years, the engineer decided to carry out both the vulnerability scans and the elimination of the security gap with our software. His aim was to automate the processes to fix the vulnerability quickly and reliably without interrupting production operations.

LOG4SHELL: PATCHING WITHOUT REBOOT

To address the Log4Shell vulnerability, the engineer and the professional services team at ondeso developed two operations, meaning automated workflows. First, they identified which of the 2,000 OT clients were affected. ondeso SR specifically scanned for vulnerability indicators and documented the impacted clients and archives in the ondeso database. Out of the 2,000 clients, around 150 were found to be affected. The subsequent operation involved several steps: First, a backup of the affected applications was created, and if necessary, write protection filters or security configurations were temporarily disabled. The patch was then copied from a network share and installed. Thanks to internal variables in ondeso SR, the connection setup could be defined generically and interpreted client-specifically. This allowed for flexible handling without needing to modify the entire operation, speeding up the initial setup and simplifying future maintenance.

After the installation, the resources used were cleaned up, and the results were updated in the database. The patching was carried out without requiring a reboot of the machines, ensuring uninterrupted operations. Some OT clients were patched immediately, while for others, an appropriate maintenance window was scheduled.

AT A GLANCE

SECTOR

Automotive industry

REQUIREMENTS

Fast and automated patching of the Log4Shell vulnerability (CVE-2021-44228) on production-critical OT clients

SOLUTION

Automated vulnerability scans and patch management by ondeso SR

100 %
AUTOMATED PROCESSING

DETAILED REPORTS AT THE TOUCH OF A BUTTON

CLOSING VULNERABILITIES WITHIN 15 MINUTES

PATCHING IN RECORD TIME

With the use of ondeso SR, the Log4Shell vulnerability was swiftly addressed. Andreas Decker, OT consultant at ondeso, says: "After successfully testing the operation, we were able to fix the vulnerability within 15 minutes. Other sites can now use this operation as well."
Thanks to ondeso SR, the cybersecurity engineer was able to efficiently resolve the issue, as the automated solution saved significant time and reduced potential sources of error. Additionally, the comprehensive reports provided a clear overview of the progress and results of the patching process.

Andreas Decker
OT consultant at ondeso

„After successfully testing the operation, we were able to fix the vulnerability within 15 minutes.“

ondeso

ondeso develops software products especially in the field of operational technology and Industry 4.0 and supports the automation of OT client management in production. For years, plant operators as well as machine and plant manufacturers have trusted in ondeso products, which are are suited for all industries and can be used across the entire range of production systems and processes. Whether management systems, HMIs or controls – ondeso manages the lifecycle of industry PCs and offers custom fitted products on the highest technological and conceptual level – 100% made in Germany.

Do you want to make the client management of your industrial PCs more efficient?

Contact us now and arrange a free software demo to get an idea of ondeso SR.

Website: www.ondeso.com/en/contact
E-Mail: contact@ondeso.com
Phone: +49 941 462932-0