DEUTSCHE GESELLSCHAFT FÜR
CYBERSICHERHEIT

Detecting Log4shell vulnerability with cyberscan.io®

With our security tool cyberscan.io® you can now scan your system for the critical Log4shell vulnerability. Below we explain how cyberscan.io® proceeds

1

Our regular scans from **cyberscan.io®** currently use several tests to identify the Log4shell vulnerability in systems. These tests all follow the same pattern.

cyberscan.io® currently tests for HTTP, SIP, TCP & UDP connections.
The scanner opens a random port between 0 & 65536 - depending on the current test differentiated between TCP & UDP.

After that, the scanner constructs the LDAP string as payload with its own external IP and the opened port as a callback address.

As an example:
payload = *„${jndi:ldap://“ + ownip + „:“ + rnd_port + „/a}“;*

Then **cyberscan.io®** injects this string into various requests, which are most likely to be logged on the server side, and waits to see if the target reports back on the opened port.

- For HTTP requests, **cyberscan.io®** uses the URL, the „referer“ and the „user agent“ to inject the payload.
- For SIP requests we use the „User-Agent“ as well as the „Contact“ field.

Finally, the scanner waits 5 seconds at a time for a request on the previously opened port. If there is a response within this time, we consider this as a hit and it is most likely that your system is affected by the Log4shell vulnerability. **A reload of further code does not take place!**

It should also be mentioned that the four different protocols (HTTP, SIP, TCP & UDP) each listen on different ports, so that an assignment is possible and can be displayed accordingly. In this way, you get clues as to which service is affected.

2

In addition to the regular rescans via **cyberscan.io®**, we will automatically scan all our customers via the tool in the coming days to check whether they are affected by the Log4shell vulnerability. Here, all externally accessible IP addresses of the customer will be specifically checked.

This automated scan works with custom DNS & LDAP servers as well as tokens for mapping. Earlier this week we provided a first script which used the canarytoken.com service as callback. In the meantime, however, we are using completely custom services here.

The mass scan will use significantly more headers, cookies and frequently used POST parameters, and will also try to get past the filters of a web application firewall (WAF).

If you need assistance with anything beyond this, we are always happy to help.

Stay safe!
Your DGC Team

Deutsche Gesellschaft für Cybersicherheit mbH & Co.KG
Geschäftsführer: Matthias Nehls
Am Fördeufer 1b
DE-24939 Flensburg

T +49.461.995 838 0
F +49.461.995 838 99

info@dgc.org
www.dgc.org