Netcontrol Security Advisory – Apache Log4j2 CVE-2021-44228

Summary

A critical vulnerability in Apache logging component has been found. The component is widely in use in a lot of software.

Affected Netcontrol products

Netcon 3000 system versions 8.0, 9.0 and 10.0, where VMware vCenter is installed.

Not affected Netcontrol products:

All other Netcontrol products, for example:

- Netcon 3000 system earlier versions (7.3, 7.2, 7.1, 7.0, 6.3, 6.2, 6.1)
- All RTU products (Netcon 500, Netcon 200, Netcon 100, RTU28, RTU8, FastNet, ….)
- Netcon Application Manager
- Netcontrol data radios and CCUs
- Netcontrol actuators

Impact on affected products

WMvare vCenter application used in some Netcon 3000 systems are affected. WMvare vCenter is a WMvare virtual environment management tool, and is used in some Netcon 3000 installations.
Affected VMvare vCenter versions are 6.5, 6.7 and 7.0. These have been used with Netcon 3000 versions 8.0, 9.0 and 10.0.

However, exploiting this vulnerability in Netcon 3000 system requires access to vCenter user interface. Access to vCenter from outside Netcon 3000 system is blocked by default. That decreases the risk considerably.

Further information

Further information can be found on

- https://nvd.nist.gov/vuln/detail/CVE-2021-44228
- https://kb.vmware.com/s/article/87081

Generic Mitigation

VMware suggest a workaround to be implemented.

Mitigation on Netcon 3000 system

A patch implementing the VMware workaround has been released by Netcontrol and sent to all customers affected by the vulnerability.

Further information can be received from Netcontrol support.

Revision history

Version	Date	Revision
1	2021-12-13	Initial version
2	2021-12-20	Not affected products added