Security Advisory Amnesia:33

Amnesia:33 refers to a collection of vulnerabilities in the modular open-source TCP/IP stacks *uIP, Nut/Net, picoTCP* and *FNET*. Since a TCP/IP stack is the first instance to process all network data, programming errors make corresponding devices vulnerable to various attack scenarios.

In the case of Amnesia:33, the stacks could be misused for Denial-of-Service (DoS) attacks with specially prepared data packets. In addition, confidential information could be tapped or the data traffic could be redirected to a domain of the attacker (DNS cache poisoning). On some devices, the vulnerabilities hold the potential for unauthorized Remote Code Execution (RCE), which could allow attackers to take control and use the device as a gateway into the network.

The security vulnerabilities were discovered by the expert company Forescout at the end of 2020. The U.S. CERT Coordination Center (CERT/CC) and the Security Agency CISA have published corresponding Security Advisories providing an overview of vulnerable and secured stack versions and also name some affected manufacturers. Please also note corresponding notifications from the Bundesamt für Sicherheit in der Informationstechnik (BSI).

A complete overview of all 33 vulnerabilities with technical details can be found in the Forescout Report on Amnesia:33. Also note the publications of Mitre Corporation, which has assigned the following CVE numbers for the particularly critical RCE vulnerabilities:

- CVE-2020-24336 (CVSS-Score 9.8/“Critical“, RCE, uIP)
- CVE-2020-24338 (CVSS-Score 9.8/“Critical“, RCE, picoTP)
- CVE-2020-25111 (CVSS-Score 9.8/“Critical“, RCE, Nut/Net)
- CVE-2020-25112 (CVSS-Score 8.1/“High“, RCE, uIP)

No Endangerment

Dallmeier recording systems and cameras are equipped with a hardened and highly adapted **LTS Linux operating system** with regard to system security. Instead of the vulnerable (modular) open source stacks, the **network stack of the respective LTS Linux kernel** is always used. Therefore, Dallmeier recording systems and cameras are **not exposed** to any vulnerabilities from the der Amnesia:33 collection.

Endangerment

Forescout experts estimate that at least 150 manufacturers and millions of devices are vulnerable to Amnesia:33. Thus, apart from Dallmeier recording systems and cameras, **all other components of a video system** are at risk, such as:

- Servers
- Routers
- Switches
- 3rd party network cameras

Dallmeier products and third-party products purchased through Dallmeier are always delivered with the latest updates and security patches at the time of shipment.

Procedure

Generally, **all components of a video system** should always be kept **up to date** with updates and security patches. Dallmeier recommends checking the components used in the systems and comparing them with the manufacturer lists, the Security Advisories of the CERT Coordination Center (CERT/CC) and the Security Agency CISA. In addition to promptly applying existing updates, the following general Forescout Experts’ Recommendations should be observed to minimize the Amnesia:33 risk:

- Disable or block IPv6 traffic if not needed
- Configure devices to use internal DNS servers
- Closely monitor external DNS traffic
- Check all network traffic for erroneous data packets (e.g. field lengths, checksums)
- Alert and block unusual network traffic

At present, corresponding updates and patches are already offered. If necessary, note the current information from the relevant manufacturers.