Security Advisory Amnesia:33

Amnesia:33 bezeichnet eine Sammlung von Schwachstellen in den modularen Open-Source TCP/IP-Stacks *uIP, Nut/Net, picoTCP* und *FNET*. Da ein TCP/IP-Stack als erste Instanz alle Netzwerkdaten verarbeitet, machen Programmierfehler entsprechende Geräte für verschiedene Angriffszenarien verwundbar.

Im Fall von Amnesia:33 könnten die Stacks mit speziell präparierten Datenpaketen für Denial-of-Service (DoS)-Angriffe missbraucht werden. Zudem könnten vertrauliche Informationen abgegriffen werden oder der Datenverkehr zu einer Domain des Angreifers umgeleitet werden (DNS cache poisoning). Auf manchen Geräten bergen die Schwachstellen das Potenzial zur unbefugten Codeausführung aus der Ferne (Remote Code Execution, RCE), wodurch Angreifer die Kontrolle übernehmen und das Gerät als Einfallstor ins Netzwerk missbrauchen könnten.

Die Sicherheitslücken wurden vom Experten-Unternehmen Forescout Ende 2020 entdeckt. Das US-amerikanische CERT Coordination Center (CERT/CC) und die Sicherheitsbehörde CISA haben entsprechende Security Advisories veröffentlicht, die einen Überblick über verwundbare und abgesicherte Stack-Versionen geben und außerdem einige betroffene Hersteller nennen. Beachten Sie auch entsprechende Meldungen des Bundesamt für Sicherheit in der Informationstechnik (BSI).

Eine Gesamtübersicht über alle 33 Schwachstellen mit technischen Details kann dem Forescout Report zu Amnesia:33 entnommen werden. Beachten Sie zudem die Veröffentlichungen der Mitre Corporation, die folgende CVE-Nummern für die besonders kritischen RCE-Lücken vergeben hat:

- 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)

Keine Gefährdung

Dallmeier Aufzeichnungssysteme und Kameras sind mit einem in Hinblick auf die Systemsicherheit stark angepassten und abgeschotteten (hardened) **LTS-Linux Betriebssystem** ausgestattet. Statt der verwundbaren (modularen) Open-Source-Stacks wird immer der **TCP/IP-Netzwerk-Stack des jeweiligen LTS-Linux Kernels** verwendet. Daher besteht **keine Gefährdung** von Dallmeier Aufzeichnungssystemen und Kameras über die Schwachstellen aus der Amnesia:33 Sammlung.

Gefährdung

Die Experten von Forescout schätzen, dass mindestens 150 Hersteller und Millionen von Geräten für Amnesia:33 anfällig sind. Abgesehen von Dallmeier Aufzeichnungssystemen und Kameras sind damit **alle weiteren Komponenten eines Videosystems** gefährdet, wie beispielsweise:

- Server
- Router
- Switches
- 3rd Party Netzwerkkameras

Dallmeier Produkte und über Dallmeier bezogene Fremdprodukte werden immer mit den zum Zeitpunkt des Versands aktuellen Updates und Sicherheits-Patches ausgeliefert.

Maßnahmen

Grundsätzlich sollten **alle Komponenten eines Videosystems** mit Updates und Sicherheits-Patches immer auf dem **aktuellen Stand** gehalten werden. Dallmeier empfiehlt die in den Systemen eingesetzten Komponenten zu prüfen und mit den Herstellerlisten, den Security Advisories des CERT Coordination Center (CERT/CC) und der Sicherheitsbehörde CISA abzugleichen. Neben dem zeitnahen Einspielen vorhandener Updates sollten folgende allgemeine Empfehlungen der Experten von Forescout zur Minimierung des Amnesia:33 Risikos beachtet werden:

- Deaktivierung oder Blockade von IPv6-Traffic sofern nicht benötigt
- Konfigurieren der Geräte für die Nutzung interner DNS-Server
- Genaue Überwachung des externen DNS-Traffic
- Prüfung des gesamten Netzwerkverkehrs auf fehlerhafte Datenpakete (z. B. Feldlängen, Prüfsummen)
- Alarmierung und Blockierung ungewöhnlichen Netzwerkverkehrs

Zum aktuellen Zeitpunkt werden entsprechende Updates und Patches bereits angeboten. Beachten Sie gegebenenfalls die aktuellen Informationen der relevanten Hersteller.