BSI

Open-Source-Code auf dem Prüfstand

[09.08.2023] Cyber-Angriffe lassen sich in den meisten Fällen auf Fehler im Programmcode der betroffenen Anwendungen zurückführen. Das Projekt CAOS will dazu beitragen, häufige Schwachstellen und Risiken zu ermitteln und zu beseitigen.

Im Rahmen eines Projekts zur Codeanalyse von Open Source Software hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) Videokonferenzsysteme und eID-Templates auf deren Sicherheitseigenschaften untersucht. Gestartet war das Projekt CAOS – kurz für: Codeanalyse von Open Source Software – bereits im Jahr 2021. Das BSI kooperierte dazu mit dem Software-Sicherheitsunternehmen mgm security partners. Aufgabe des Projekts ist die Schwachstellenanalyse mit dem Ziel, die Sicherheit von Open Source Software zu erhöhen. Das Projekt soll Entwicklerinnen und Entwickler bei der Erstellung sicherer Software-Anwendungen unterstützen und das Vertrauen in Open Source Software steigern, berichtet das BSI. Der Fokus liegt auf Anwendungen, die vermehrt von Behörden oder Privatanwendern genutzt werden.

BSI und mgm security partners überprüften den Quellcode der Videokonferenzsysteme BigBlueButton und Jitsi auf mögliche Mängel. Kritische Schwachstellen hat das BSI den betroffenen Entwicklern sofort mitgeteilt – diese konnten die gefundenen Sicherheitslücken schnell beheben. Weitere Mängel wurden im Rahmen eines Responsible-Disclosure-Verfahren adressiert. Bei den nun veröffentlichten Ergebnissen handelt es sich um eine Kombination aus Sourcecode Review, dynamischer Analyse und Schnittstellenanalyse in den Bereichen Netzwerkschnittstellen, Protokolle und Standards.

Die ebenfalls untersuchten eID-Templates sind Teil der geplanten Einführung der eID-Card, der neuen Chipkarte mit Online-Ausweis, mit der sich Bürgerinnen und Bürger bei Inanspruchnahme digitaler Dienstleistungen authentifizieren können. eID-Templates sollen es verschiedenen Diensteanbietern – namentlich WordPress und Nextcloud – erleichtern, ein solches Authentifizierungsangebot in ihre Infrastruktur zu integrieren.

Um die Sicherheit von Open Source Software in Zukunft zu erhöhen, sind weitere Codeanalysen geplant. Das Projekt zur Codeanalyse von Open Source Software wird unter dem Namen CAOS 2.0 fortgeführt. Die Ergebnisse sollen nach einem Responsible-Disclosure-Verfahren ebenfalls auf der Website des BSI veröffentlicht werden. Das Verfahren gestattet Entwicklern eine angemessene Frist zur Behebung von Sicherheitslücken vor deren Veröffentlichung.

(sib)

Codeanalyse Videokonferenzsysteme – Ergebnisse (PDF; 3,9 MB)
Codeanalyse eID-Templates (PDF; 1,4 MB)

Stichwörter: IT-Sicherheit, BSI, mgm security partners, Open Source Software, CAOS