Contribution ID: **27** Type: **Paper presentation**

Security Audit for the D Programming Language

Friday 5 November 2021 16:20 (20 minutes)

Memory corruption has been, traditionally, the number one cause for software vulnerabilities. As a consequence, programming languages that offer automated, compile time memory safety checks have been developed, such as D and Rust. However, since programming languages are pieces of software, they also may suffer from vulnerabilities that may be exploited to bypass the memory safety checking algorithm.

In this paper, we perform a security audit of the D programming language. Our findings uncover security holes in the D safety checking system. We show
that it is possible to escape expired stack pointers which can be used to ultimately execute arbitrary code. In addition, we discuss and implement potential fixes to the discovered issues.

Authors: NITU, Razvan (University POLITEHNICA of Bucharest); STANILOIU, Constantin Eduard (University POLITEHNICA of Bucharest); DONE, Cristian (University POLITEHNICA of Bucharest); RUGHINIȘ, Răzvan Victor (University Politehnica of Bucharest)

Presenter: NITU, Razvan (University POLITEHNICA of Bucharest)

Session Classification: Network Security && Pervasive Systems and Computing

Track Classification: Network Security