

# The use of vulnerability data for risk assessment

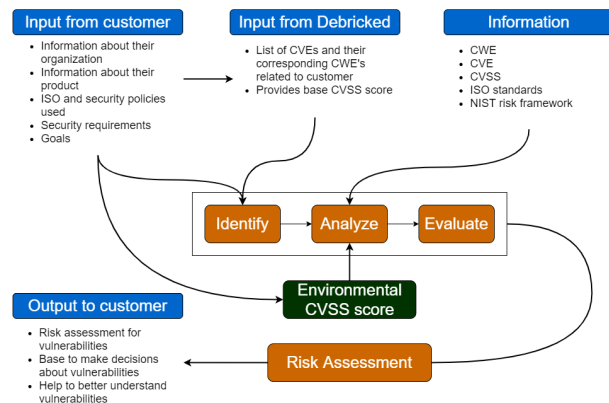
## POPULÄRVETENSKAPLIG SAMMANFATTNING Jenny Martinsson

Cyber threat is one of the biggest global risk sources right now according to the World Economic Forum. Cyber threat can take many different forms, which leads to cybersecurity being a very extensive area. In this report we look at vulnerabilities in open sourced code and how they can be used to make a risk assessment.

Finding and recording vulnerabilities in open sources code is something that is well maintained, and there are several big databases out there which gather all the known vulnerabilities. They often use a scoring system, called CVSS (Common Vulnerability Scoring System) which gives an idea of how severe a vulnerability can be. The CVSS is however not a perfect system, and many people see the CVSS score as a risk assessment for a vulnerability. This is not true however, since it only measures severity. To amend this the base CVSS score has two optional parts in their scoring system, called temporal score and environmental score. In this paper we focus on the environmental score, which is used to put the vulnerability in a specific context. The environmental score is furthermore divided into two parts, security requirements and modified base metrics.

Our first step was to help people figure out their security requirements. In the next step we showed how easily the modified base metrics can be changed depending on what system they are used on. The last thing we did was to put the vulnerabilities in a larger risk perspective. To do this we used ISO 27002 which is a set of guidelines for information security requirements. We used the ISO controls and made a connection between them and some vulnerabilities, to show how the vulnerabilities can affect you.

Our goal is to help organisations make decisions about vulnerabilities they have in their software programs by helping them make their own risk assessments. We also hope that the outcome of this master thesis will contribute to how we can use the CVSS score and other information security properties to make risk assessments easier and getting people to look at cybersecurity from a bigger risk perspective.



Our conclusion shows that it is important to look at vulnerabilities from a bigger risk perspective, and that our method can be of help when making continuous risk assessments in cybersecurity since a lot of the data can be reused when doing future risk assessments.