Abstract

• Infrastructure as code (IaC) is the practice of automatically managing configurations following the recommended software development practices.

• In our research, we investigate if insecure coding patterns (ICPs) in IaC scripts are propagated from one repository to multiple repositories in the open source software (OSS) ecosystem.

Research Objective

The goal of this project is to help practitioners secure configuration scripts by characterizing propagation of insecure coding patterns.

Background

• We use a tool called Security Linter for Infrastructure as Code (SLIC) [1] to analyze and identify ICPs in repositories that are cloned from other repositories.

• We compare the resulting output from the SLIC tool to determine the propagation of ICPs for IaC scripts in OSS.

Detected Types of ICPs

• Admin by default
• Empty password
• Hard-coded secret
• Invalid IP address binding
• Suspicious comment
• Use of HTTP without TLS
• Use of weak cryptography algorithms

Problem Statement

Despite the popularity of IaC tools, insecure coding patterns (ICPs), such as hard-coded passwords, can be unintentionally introduced into IaC scripts, which eventually can propagate across other repositories with IaC scripts.

Methodology

• Fetch the Forked Repositories from the Main Repository Name
• Clone the Main Repository and Forked Repositories
• Run the SLIC Tool on the Main Repo and its Forked Repos to identify possible ICPs
• Compare SLIC Tool output from the Main Repo to that of its Forked Repos to identify propagating ICPs
• Graph the relationships of ICPs between the Main Repo and Forked Repositories

Graphs

Graphing

Comparison Process

Analysis CSV

Visualization of comparison process from SLIC Tool Output

Git Clone File Structure

Visualization of file storage structure for automated git-cloning.

Table of Results

<table>
<thead>
<tr>
<th>Forks</th>
<th># of Original ICPs</th>
<th># of Propagated ICPs</th>
<th>% of ICPs Propagated</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>31</td>
<td>5</td>
<td>153</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>492</td>
<td>467</td>
</tr>
<tr>
<td>3</td>
<td>30</td>
<td>2</td>
<td>60</td>
</tr>
</tbody>
</table>

Based on preliminary findings we recommend practitioners take the utmost security consideration for ICPs in IaC scripts as they can propagate from one repository to another, creating large-scale propagation of ICPs in the OSS IaC ecosystem.

Next Steps

• Repeat the process for a larger dataset
• Perform a manual comparison to verify results
• Refine the tool to perform a more in-depth search
• Identifying Multi-Level ICP Propagation through forks

References


We would like to thank Dr. Akond Rahman and Department of Computer Science at Tennessee Technological University.