ABSTRACT

The Linux kernel is quickly evolving and extensively customized. This results in thousands of versions and derivatives. Unfortunately, the Linux kernel is quite vulnerable. Each year, thousands of bugs are reported, and hundreds of them are severe vulnerabilities. Given the limited resources, the kernel maintainers have to prioritize patching the more severe vulnerabilities. In practice, the Common Vulnerability Scoring System (CVSS) [1] has become the standard for characterizing vulnerability severity. However, a fundamental problem exists when CVSS meets Linux—it is used in a “one for all” manner. The severity of a Linux vulnerability is assessed for only the mainstream Linux, and all affected versions and derivatives will simply honor and reuse the CVSS score. Such an undistinguished CVSS usage results in underestimation or overestimation of severity, which further results in delayed and ignored patching or wastes of the precious resources. In this paper, we propose OS-aware vulnerability prioritization (namelyDIFFCVSS), which employs differential severity analysis for vulnerabilities. Specifically, given a severity-assessed vulnerability, as well as the mainstream version and a target version of Linux, DIFFCVSS employs multiple new techniques based on static program analysis and natural language processing to differentially identify whether the vulnerability manifests a higher or lower severity in the target version. A unique strength of this approach is that it transforms the challenging and laborious CVSS calculation into automatable differential analysis. We implement DIFFCVSS and apply it to the mainstream Linux and downstream Android systems. The evaluation and user-study results show that DIFFCVSS is able to precisely perform the differential severity analysis, and offers a precise and effective way to identify vulnerabilities that deserve a severity reevaluation.
Poster: OS-Aware Vulnerability Prioritization via Differential Severity Analysis

Qiushi Wu\textsuperscript{1}, Yue Xiao\textsuperscript{1}, Kangjie Lu\textsuperscript{2}
(\textsuperscript{*} co-first authors)

Abstract
The severity of a Linux vulnerability is assessed for only the mainstream Linux, and most affected versions and derivatives will simply honor and reuse the CVSS score. Such an undistinguished CVSS usage results in underestimation or overestimation of severity, which further results in delayed and ignored patching or wastes of the precious resources. In this paper, we propose OS-aware vulnerability prioritization (namely DIFFCVSS), which employs differential severity analysis for vulnerabilities.

Introduction
A fundamental problem arises when CVSS meets Linux — it is used in an “one for all” manner. When a bug reporter requests a CVE for a vulnerability, the CVE maintainers assign a (single) CVSS score for it, typically based on the mainstream Linux. All affected versions and some derivatives will then simply honor the assigned CVSS score for prioritizing their patches. This is understandable because assigning the CVSS score is quite laborious and requires expertise. Maintainers of small derivatives may not afford the reevaluation for all of their system. However, this results in both severity overestimation which wastes maintenance resources and severity underestimation which delays the patching of critical vulnerabilities and incurs critical threats.

To address it, we present DIFFCVSS, a system that can automatically and precisely determine if a vulnerability will have a higher or lower severity in a different OS. DIFFCVSS incorporates multiple new techniques, such as automatically identifying the call-chain for a vulnerability and mapping kernel functions to CVSS metrics, to ensure precision and effectiveness.

Methodology
1. Mapping Metrics to Functions
2. Recognize Vulnerability Artifact
3. Identify Vulnerability Call-Chain
4. Differential Severity Analysis

Evaluation
Q1: How efficient is DIFFCVSS in reducing maintainer workload?
Q2: How accurate is DIFFCVSS in re-evaluating vulnerability?
Q3: How usable is DIFFCVSS in practice?

- DIFFCVSS can save 91.98% of time, reduce 76.7% of workload
- DIFFCVSS achieves an accuracy of 89.53% in Metric-level and 90.6% in Severity-level on average.

Findings
- 110 vulnerabilities that have different severity across Android and Linux.
- 18 of them have a higher severity and should be reevaluated per OS to avoid delayed patching.

<table>
<thead>
<tr>
<th>OS Combination</th>
<th># Vulnerabilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>More severe in Android</td>
<td>13</td>
</tr>
<tr>
<td>More severe in Linux</td>
<td>63</td>
</tr>
<tr>
<td>Similar severe in Linux and Android</td>
<td>51</td>
</tr>
</tbody>
</table>

Table 7: Cross-OS vulnerability exploitability metric difference between Linux and Android.

Conclusions
- The “one for all” strategy results in both severity overestimation and severity underestimation.
- We propose a system that can automatically and precisely determine if a vulnerability will have a higher or lower severity in a different OS.