Carnegie Mellon University
Software Engineering Institute

CERT Coordination Center Comments on DHS Vulnerability Discovery Program, 1601-0028

Docket Number DHS-2021-0009

Background

The CERT Coordination Center (CERT/CC) is part of the Software Engineering Institute (SEI) at Carnegie Mellon University. One focus area of the CERT/CC is the analysis, coordination, disclosure, and remediation of software vulnerabilities. This work dates back to the origin of the CERT/CC in 1988[1] and our comments are based on both practical experience and experimental research. The SEI is a DoD-sponsored FFRDC.

The following comments are respectfully submitted to the Department of Homeland Security for consideration and inclusion in the upcoming version of DHS agency Information Collection Activities: Vulnerability Discovery Program, 1601-0028 in support of section 101 of the Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act (SECURE Technology Act).

For questions about these comments please contact Laurie Tyzenhaus <latyzenhaus@cert.org>.

[1] http://www.mycal.net/Group42/hack/unix/cert/ca-88.01

Summary

The SECURE Technology Act encourages individuals, organizations, and companies to submit any security vulnerabilities found associated with the civilian U.S. Government information systems of . The comments in this document address DHS' request for what information should be included in a vulnerability report.

While not specifically requested, our comments provide some detail on what elements should be considered for inclusion in a vulnerability reporting form.

A vulnerability report should result in an action taken by the organization receiving the report. The report should include actionable information, a researcher contact, and provide enough details to allow the defender to take action. In the following sections, CERT/CC details the information which should be collected to defend U.S. Government systems.

Vulnerability Reporting

Actionable Information: Vulnerability Description

A security defender needs detailed information to mitigate or remediate the vulnerability. Once the vulnerability has been confirmed and addressed, the security defender should identify any other systems which may also be vulnerable. If required, the defender should report back to their Agency the mitigating results and the number of systems fixed.

An actionable vulnerability report should include:

1. Version number of the product or software affected.
2. The URL, IP address, and any other identifiable information.
3. Identify the CWE[2] (Common Weakness Enumeration) or provide a description of the weakness.
4. Provide a detailed technical description of the vulnerability, including proof of concept if possible. Make it easy for the report recipient to be able to test and confirm the existence of the vulnerability.
5. An explanation of how the vulnerability could be exploited by an attacker. A description of other conditions necessary for the attack to work.
6. Identify the Federal Agency affected. Identify any other Federal Agencies affected. As many systems and applications may be used by multiple agencies, an indication that multiple agencies are affected is important information.
7. A description of what the attacker gains by exploiting the vulnerability. An explanation of the impact to the system and the information stored.
8. Estimate the severity of this issue. Provide a range of possible options.
9. List the CVE[3] (Common Vulnerabilities and Exposures) number, if known. CVE IDs typically do not exist for non-public vulnerability reports.
10. A description of tools or techniques used to discover the vulnerability
11. An option to upload a file to provide additional information.
12. A determination of the public knowledge and indications of active exploitation. If the vulnerability is not public, the researcher may be planning to publicly disclose the vulnerability. The disclosure may occur at a conference, on a security blog or in a research paper. Inquire if the researcher has any deadlines to submit a paper or plans to publish.

For a current production example, see our vul report form:
https://kb.cert.org/vuls/vulcoordrequest/

[2] CWE is a community-developed list of software and hardware weakness types. (https://cwe.mitre.org)
[3] CVE is a list of publicly disclosed computer security flaws, records each containing an identification number, description and public reference. (https://cve.mitre.org)

Researcher Contact

The researcher should provide contact information which will allow the defender to interact and ask questions. The researcher may desire anonymity and insist on using a proxy, freely available email address and/or a pseudonym, alias, or handle in place of a real name.

Ask the researcher if they wish to be acknowledged by name in any published document about this vulnerability.

The experienced researcher will be comfortable with providing the above information, as many public and private bug bounty programs already request contact information. A less experienced researcher may scoff at the request for contact information, however the ability to report anonymously will encourage contributions.