No Action Required? CVE for Software as a Service

Art Manion

Don “Beetle” Bailey (AWS)

Lisa Olson (Microsoft)

Michael Cote (Google)

Background

- Vulnerability (risk) remediation, mitigation, management
- Security fixes for software-as-a-service are typically performed by the provider and can be deployed quickly and with full coverage
- The CVE Numbering Authority (CNA) Operational Rules address this, there was a change from 3.0 to 4.0 (effective August 2024)
- Let’s talk to some SaaS providers!

The Rules, 3.0

7.4.4 CNAs MAY assign a CVE ID to a vulnerability if:

a. The product or service is owned by the CNA,

b. The product or service is not customer controlled, and

c. The vulnerability requires customer or peer action to resolve.

7.4.5 CNAs MUST NOT assign a CVE ID to a vulnerability if the affected product(s) or service(s):

a. Are not owned by the CNA, and

b. Are not customer controlled.

7.4.6 CNAs MAY assign a CVE ID to a vulnerability if the affected product(s) or service(s):

a. Are not owned by the CNA and

b. Are customer controlled.

The Rules, 4.0

4.2.2.2 CNAs SHOULD Publicly Disclose and assign a CVE ID if the Vulnerability:

1. has the potential to cause significant harm, or
2. requires action or risk assessment by parties other than the CNA or Supplier.

4.2.2.3 CNAs MAY Publicly Disclose Vulnerabilities for other reasons.

4.2.3 CNAs MUST NOT consider the type of technology (e.g., cloud, on-premises, artificial intelligence, machine learning) as the sole basis for determining assignment.

5.1.11.1 MUST use the "exclusively-hosted-service" tag when all known Products listed in the CVE Record exist only as fully hosted services. If the Vulnerability affects both hosted services and on-premises Products, then this tag MUST NOT be used.

Rough Counts


```
$ grep -ri exclusively-hosted-service cvelistV5/cves/ | wc -l
      51
```