Intellectual Property & Technology Law Journal

Edited by the Technology and Proprietary Rights Group of Weil, Gotshal & Manges LLP

VOLUME 33 • NUMBER 9 • OCTOBER 2021

Tracking Hacks: A Primer on Software Vulnerability Databases and Recent High-Stakes Litigation

Andrew Wilson

It is hard to turn on the news without hearing about yet another high profile ransomware attack or data breach impacting our nation's security, supply chains, and infrastructure. Indeed, experts estimate that between 2019 and 2020, ransomware attacks rose by 62 percent worldwide, and by 158 percent in North America alone.[1]

The recent and dramatic rise in cyberattacks is particularly difficult to ignore for those responsible for securing critical software systems, who are frantically trying to avoid becoming the next cybersecurity headline. It is no surprise then that President Biden's Executive Order on Improving the Nation's Cybersecurity (May 12, 2021) calls for immediate action to counter the "persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy."[2]

VULNERABILITY DATABASES

What is less publicized, however, is the complex world of both public and proprietary cybersecurity systems known as "vulnerability databases" that aim to secure the reusable software components we rely on. This article provides an introduction to vulnerability databases and shines a light on some pending litigation that could have a big impact on the cybersecurity industry.

One way hackers can gain access to sensitive systems is by exploiting a security vulnerability, or bug, in the software. The National Vulnerability Database ("NVD") is a U.S. government-sponsored repository of standards-based vulnerability management data managed by the National Institute of Standards and Technology ("NIST").[3]

One way hackers can gain access to sensitive systems is by exploiting a security vulnerability, or bug, in the software.

The NVD includes a free, open database of security checklist references, security-related software flaws, misconfigurations, product names, and impact metrics – information that can be used to identify and remediate critical vulnerabilities in reusable software.[4] Software vendors can use this information to publish patches or issue configuration guidance to NVD itself if necessary.

Andrew Wilson, a senior associate in the Washington, D.C., office of Baker Botts L.L.P., focuses his practice on high-tech patent litigation involving complex technologies. He may be contacted at *andrew.wilson@bakerbotts.com*.

However, there has been a longstanding gap between the number of vulnerabilities discovered and those tracked in NVD. Some estimate that there are between 30 percent to 50 percent more known vulnerabilities than those that are identified in NVD, and many entries are estimated to be inaccurate or incomplete.[5] Thus, organizations tend to struggle to keep their software secure through NVD alone.

Most of the information in NVD comes from the Common Vulnerabilities and Exposures ("CVE") Program, which is a related, government-sponsored program.[6] In order to ensure the integrity of the vulnerability identification process, only an exclusive set of organizations – called CVE Numbering Authorities, or CNAs – are invited to report, verify, and maintain this publicly accessible information on identified vulnerabilities.[7]

Typically, CNAs are software vendors that focus on assigning identifiers ("CVE IDs") to newly discovered vulnerabilities within software they have developed (e.g., Red Hat identifies "vulnerabilities in open-source projects affecting Red Hat offerings . . .," and Microsoft covers "Microsoft issues only.").[8] It is in the software vendor's best interest to publicly report vulnerabilities so that downstream users of their software are put on notice and can take remedial measures.

REPORTING OBLIGATIONS

Recently, however, the NVD and CVE sponsors appointed Synopsys Software Integrity Group ("SIG") as a CNA – i.e., an entity responsible for reporting vulnerabilities to the free and publicly accessible CVE and NVD vulnerability databases.[9] This is notable because of Synopsys SIG's affiliation with Synopsys' wholly-owned subsidiary Black Duck Software, which provides a proprietary vulnerability database and source code scanning and auditing products focusing on embedded open source software.[10]

Synopsys SIG's public vulnerability reporting obligations as a CNA may create a tension with Black Duck's proprietary vulnerability database. Synopsys' reporting responsibilities include "vulnerabilities in third-party software discovered by Synopsys SIG that are not in another CNA's scope," which could potentially include proprietary vulnerability information.[11] And Synopsys recently suggested that it may already be contributing some of its proprietary "research" on vulnerabilities to CVE/NVD as a responsible CNA and "good steward of the broader software ecosystem."[12] In fact, Synopsys states that it will help CVE and NVD to "close that gap" of 30 percent to 50 percent in unreported vulnerabilities.[13]

These statements caught the attention of Risk Based Security Inc. ("RBS"), which licensed its allegedly proprietary vulnerability database called "VulnDB" to Black Duck in 2015 for use in the Black Duck Hub cloud scanning suite.[14] RBS is currently engaged in two lawsuits with Black Duck and Synopsys over the origin and ownership of Black Duck's purportedly proprietary vulnerability information.

First, in 2018, RBS filed a lawsuit against Black Duck in Massachusetts state court alleging that Black Duck was infringing its trade secret security vulnerability information from RBS's VulnDB through a product called Black Duck Hub.[15] Many of the filings in this case are sealed, but it appears that Black Duck is challenging the proprietary nature of the information in VulnDB, contending that it is not protectible trade secret information because it was assembled from public data sources.[16]

More recently, in response to Synopsys' statements about disclosing potentially proprietary vulnerability information to "close that gap" in reported vulnerabilities, RBS allegedly sent a cease and desist letter asking Synopsys "to refrain from identifying vulnerabilities to CVE."[17]

In response, Synopsys filed a declaratory judgment action in the Eastern District of Virginia asserting, among other things, that VulnDB is not RBS' trade secret and that Synopsys did not misappropriate VulnDB.[18] RBS filed a motion to stay this more recent federal litigation pending resolution of the overlapping trade secret matters in Massachusetts state court, but that motion was denied in a minute order on July 20, 2021, with an opinion to issue in the near future.[19]

CONCLUSION

The currently pending disputes between RBS and Synopsys/Black Duck could have significant impacts for the cybersecurity world and vulnerability databases in general. On the one hand, vulnerability information can be efficiently disseminated to downstream software users if consolidated in one publicly available repository. However, eliminating proprietary restrictions on use of that information may dis-incentivize discovery and tracking of vulnerabilities at a critical time. These cases could provide insight into how vulnerability information is treated under U.S. intellectual property law.

Notes

[1] *See https://blog.sonicwall.com/en-us/2021/03/sonicwall-exposes-soaring-threats-historic-power-shifts-in-new-report/*. Other firms estimate an even higher year-over-year increase of over 400 percent from 2019 - 2020. *See https://www.bitdefender.com/files/News/CaseStudies/study/395/Bitdefender-2020-Consumer-Threat-Landscape-Report.pdf.*

[2] *https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.*

[3] *https://nvd.nist.gov/.*

[4] *https://nvd.nist.gov/general/FAQ-Sections/General-FAQs#faqLink0.*

[5] *https://www.synopsys.com/blogs/software-security/synopsys-cve-numbering-authority/#:~:text=As%20a%20CVE%20Numbering%20Authority,software%20for%20nearly%20a%20decade.*

[6] *https://cve.mitre.org/cve/.*

[7] *https://cve.mitre.org/cve/cna.html.*

[8] *https://cve.mitre.org/cve/request_id.html#cna_participants.*

[9] *https://www.synopsys.com/blogs/software-security/synopsys-cve-numbering-authority/*; *https://cve.mitre.org/cve/request_id.html#cna_participants.*

[10] *https://manuals.plus/synopsys/black-duck-software-composition-analysis* ("Black Duck's open source security risk insight combines curated data from public sources (e.g., NVD) and detailed, proprietary analysis from the Synopsys Cybersecurity Research Center (CyRC).").

[11] *https://cve.mitre.org/cve/request_id.html#s.*

[12] *Compare https://manuals.plus/synopsys/black-duck-software-composition-analysis* ("Black Duck's open source security risk insight combines curated data from public sources (e.g., NVD) and detailed, proprietary analysis from the Synopsys Cybersecurity Research Center (CyRC).") *with https://www.synopsys.com/blogs/software-security/synopsys-cve-numbering-authority/* ("CyRC has already discovered and contributed vulnerabilities to the CVE list.").

[13] *https://www.synopsys.com/blogs/software-security/synopsys-cve-numbering-authority/.*

[14] *https://www.businesswire.com/news/home/20150407005248/en/Black-Duck-Software-and-Risk-Based-Security-Partner-to-Launch-the-Black-Duck-Hub-to-Address-Security-Vulnerabilities.*

[15] Complaint (D.I. 1) at 1, *Risk Based Security Inc., v. Black Duck Software, Inc.*, case no. 2084-cv-0258.

[16] Memorandum in Support of Defendant's Motion to Stay (D.I. 9) at 3, case no. 3:21-cv-00252 (describing Black Duck's Defenses in state court case).

[17] Memorandum in Support of Defendant's Motion to Stay (D.I. 9) at 4, *Synopsys, Inc., v. Risk Based Security*, Inc., case no. 3:21-cv-00252.

[18] Joint Status Report in Advance of May 5, 2021 Hearing at 2 (case no. 2084-cv-0258).

[19] That opinion had not yet issued at the time of publication.

Wolters Kluwer