Health-ISAC Weekly Blog -- Hacking Healthcare™

Hacking Healthcare | TLP:WHITE | Alert ID : 93be3051 | Nov 09, 2023, 02:36 PM

This week, *Hacking Healthcare*™ takes a longer look at the recent SEC compliant that was filed against SolarWinds and its former CISO, Timothy Brown. We examine what the SEC Complaint alleges and then cover a few grounded takeaways for Health-ISAC members to ponder.

Welcome back to *Hacking Healthcare*™.

AI Executive Order

Many of you are aware of the lengthy AI Executive Order recently published by the Biden administration, but if navigating the sweeping scope of the document to understand all its potential impacts on the healthcare sector sounds overwhelming, we have you covered. Next week's Hacking Healthcare is dedicated to exploring some of the general and healthcare-specific aspects Health-ISAC members should be aware of.

SEC Complaint Targets SolarWinds and its former CISO

On October 30th, the SEC published a Complaint against the "software company SolarWinds Corporation and its chief information security officer, Timothy G. Brown, for fraud and internal control failures relating to allegedly known cybersecurity risks and vulnerabilities."[i] While much of the SEC's approach is not groundbreaking, the singling out of Brown has raised serious concerns and spawned numerous thought pieces on what it means for CISOs. This piece will dive into what the SEC is charging SolarWinds with before providing some measured takeaways for Health-ISAC members.

SEC Complaint

The SEC complaint filed on October 30 alleges that "[f]rom at least October 2018 through at least January 12, 2021, Defendants SolarWinds and its then-Vice President of Security and Architecture, Brown, defrauded SolarWinds' investors and customers through misstatements, omissions, and schemes that concealed both the Company's poor cybersecurity practices and its heightened—and increasing—cybersecurity risks."[ii]

The SEC Complaint goes on to cite how "SolarWinds made materially false and misleading statements and omissions related to SolarWinds' cybersecurity risks and practices in at least three types of public disclosures."[iii] These included a security statement on the SolarWinds website, numerous S-1 and S-8 SEC forms, and a Form 8-K relating to the Orion cyber incident. Also cited were several blog posts and interviews given by Brown on various cybersecurity matters.

These public-facing statements, which generally touted SolarWinds' good cybersecurity maturity and practices, were contrasted with numerous examples of SolarWinds' internal documents and communications, which painted a very different picture of its cybersecurity maturity and its awareness of specific cyber vulnerabilities and threats related to SolarWinds products.

Some specific examples include:

Passwords: SolarWinds' public-facing security statement claimed that it had implemented a strong password policy that was enforced over "all applicable information systems, applications, and databases."[iv] According to the SEC, internal communications suggest that the password policy was not always followed. For example, the SEC cites an incident in which the password to SolarWinds' Akamai server, which was used to distribute software updates to SolarWinds' customers, had been made publicly available. The password is alleged to have been "solarwinds123."[v] In another example, one of SolarWinds' employees expressed surprise that one of its products had a default password of "password."[vi]

Secure Development Lifecycle (SDL): SolarWinds' public-facing security statement claimed that the company followed "a defined methodology for developing secure software that is designed to increase the resiliency and trustworthiness of our products," and stated: "Our secure development lifecycle follows standard security practices including vulnerability testing, regression testing, penetration testing, and product security assessments."[vii]

According to the SEC, SolarWinds knew this was not the case, and the SEC complaint alleges that in an internal email from "SolarWinds' CIO, Engineering Manager H bluntly admitted that the Security Statement's SDL section was false," and that improvements over time were needed.[viii] The SEC stated: "A plan to begin taking steps to implement an SDL is a far cry from presently employing an SDL as represented to the public in the Security Statement."[ix]

Access Controls: SolarWinds' public-facing security statement claimed that the company implemented role-based access controls, applied the concept of least privilege, and had put procedures in place to remove old or unused accounts. The SEC alleges that "SolarWinds routinely and pervasively granted employees unnecessary 'admin' rights," and that "there is evidence that most employees had 'Admin' rights at times during the Relevant Period."[x]

SEC Filings: The SEC also alleged that, in addition to concealing some of the above practices, annual and periodic SEC filings submitted by SolarWinds were too generic and discussed threats and vulnerabilities in a hypothetical manner rather than acknowledging known risks and threats. The SEC noted that SolarWinds "disclosed the same hypothetical, generalized, and boilerplate description" across the time

period assessed, despite internal communications that illustrated changing circumstances and cyber risks.

Brown's Statements: Interestingly, the SEC also cited numerous blog posts written by Brown and interviews of Brown on a variety of cybersecurity issues. The contents of the public-facing interviews and blog posts generally show Brown to be keenly aware of how important it is for organizations to follow the kinds of cybersecurity best practices that SolarWinds attested to in its security statement. The SEC's complaint suggests that Brown made these comments while aware that SolarWinds was not itself adhering to them.

There is much more within the 68-page complaint, and we encourage anyone interested to explore it in more depth.

Action & Analysis
Included with Health-ISAC Membership

Congress
Tuesday, November 7
No relevant meetings

Wednesday, November 8
No relevant meetings

Thursday, November 9
No relevant meetings

International Hearings/Meetings

[i] https://www.sec.gov/news/press-release/2023-227
[ii] https://www.sec.gov/news/press-release/2023-227
[iii] https://www.sec.gov/files/litigation/complaints/2023/comp-pr2023-227.pdf
[iv] https://www.sec.gov/files/litigation/complaints/2023/comp-pr2023-227.pdf
[v] https://www.sec.gov/files/litigation/complaints/2023/comp-pr2023-227.pdf
[vi] https://www.sec.gov/files/litigation/complaints/2023/comp-pr2023-227.pdf
[vii] https://www.sec.gov/files/litigation/complaints/2023/comp-pr2023-227.pdf
[viii] https://www.sec.gov/files/litigation/complaints/2023/comp-pr2023-227.pdf
[ix] https://www.sec.gov/files/litigation/complaints/2023/comp-pr2023-227.pdf
[x] https://www.sec.gov/files/litigation/complaints/2023/comp-pr2023-227.pdf

Report Source(s)

Health-ISAC

Reference | References

sec
Health-ISAC
sec

Tags

Regulatory, Hacking Healthcare, SEC, SolarWinds Orion, Securities And Exchange Commission, SolarWinds, regulatory sanctions

TLP:WHITE: Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

For Questions and/or Comments:

Please email us at contact@h-isac.org

Conferences, Webinars, and Summits:

https://h-isac.org/events/

Hacking Healthcare:

Hacking Healthcare is co-written by John Banghart and Tim McGiff.

John Banghart has served as a primary advisor on cybersecurity incidents and preparedness and led the National Security Council's efforts to address significant cybersecurity incidents, including those at OPM and the White House. John is currently the Senior Director of Cybersecurity Services at Venable. His background includes serving as the National Security Council's Director for Federal Cybersecurity, as Senior Cybersecurity Advisor for the Centers for Medicare and Medicaid Services, as a cybersecurity researcher and policy expert at the National Institute of Standards and Technology (NIST), and in the Office of the Undersecretary of Commerce for Standards and Technology.

Tim McGiff is currently a Cybersecurity Services Program Manager at Venable, where he coordinates the Health-ISAC's annual Hobby Exercise and provides legal and regulatory updates for the Health-ISAC's monthly Threat Briefing.

- John can be reached at jbanghart@h-isac.org and jfbanghart@venable.com.
- Tim can be reached at tmcgiff@venable.com.

Access the Health-ISAC Intelligence Portal:

Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Cyware.

For Questions or Comments:

Please email us at toc@h-isac.org