Health-ISAC Weekly Blog -- Hacking Healthcare

Hacking Healthcare | TLP:WHITE | Alert ID : 09c62f3c | Apr 14, 2023, 01:47 PM

This week, *Hacking Healthcare* provides an update on the FDA's implementation of cybersecurity requirements for medical devices that were outlined in the 2023 Consolidated Appropriations Act. Next, we take another look at supply chain security as another significant incident pushes the issue back into the headlines.

Welcome back to *Hacking Healthcare*.

FDA Provides Medical Device Cybersecurity Guidance

On March 30th, the Food and Drug Administration (FDA) published a notice on the availability of final guidance entitled, "Cybersecurity in Medical Devices: Refuse to Accept Policy for Cyber Devices and Related Systems Under section 524B of the Federal Food, Drug, and Cosmetic Act (FD&C Act)." As the name suggests, this guidance addresses the FD&C Act amendments that were made toward the end of last year. So, what does the notice mean for medical device manufacturers?

As a reminder, the 2023 Consolidated Appropriations Act contained requirements for "cyber devices" that are included in premarket submissions. These included:[i]

- Submitting a plan to monitor, identify, and address, as appropriate, in a reasonable time, post-market cybersecurity vulnerabilities and exploits, including coordinated vulnerability disclosure and related procedures

- Designing, developing, and maintaining processes and procedures to provide a reasonable assurance that the device and related systems are cybersecure

- Providing to the Secretary of HHS a software bill of materials (SBoM), including commercial, open-source, and off-the-shelf software components

It also granted explicit authorities for the FDA to implement "other requirements as the Secretary may require through regulation to demonstrate reasonable assurance that the device and related systems are cybersecure."[ii] The text of the Appropriations Act outlined that these requirements would take effect 90

days after the Act's enactment, roughly the end of March, but this new notice effectively creates an additional transitionary timeframe.

Referencing the requirements listed above, the FDA is using this notice to highlight that they generally do NOT intend to issue "refuse to accept" (RTA) "decisions for premarket submissions submitted for cyber devices based solely on information required by section 524B of the FD&C Act before October 1, 2023."[iii], [iv] The FDA instead intends to "work collaboratively with sponsors of such premarket submissions as part of the interactive and/or deficiency review process."[v] Past that date, the FDA believes that entities will have had enough time to adapt and that RTAs are more likely.

Given the relatively short time frame that FDA was given by the Consolidate Appropriations Act text, the FDA determined that it was not feasible to implement a formal public comment period on this decision. However, the FDA makes clear that despite the lack of a formal comment period, they "will consider all comments received and revise the guidance document as appropriate."[vi]

The FDA has helpfully created an accessible quick reference FAQ on this matter, which members are encouraged to review.[vii]

Action & Analysis
Included with Health-ISAC Membership

Supply Chain Cyberattacks Hit the Headlines Again

Supply chain attacks arguably broke into the national consciousness during the 2020 SolarWinds attack, an incident that had the potential to directly impact 18,000 organizations.[x] However, supply chain attacks have long predated SolarWinds and they appear to be picking up in frequency, including a recent attack on 3CX products.[xi].

3CX is a company that markets itself as a complete business communications platform, supplying solutions for millions of customers worldwide, including major companies like, Toyota, Coca Cola, and the UK's National Health System (NHS).[xii] 3CX was recently the victim of a supply chain attack in which hackers altered their communication installation software to steal credentials and other relevant information from the large companies using 3CX's software, with a specific focus on the cryptocurrency industry. This type of supply chain cyberattack is what's known as an "enabler operation" in which the hackers infiltrate a system and steal information to be used and leveraged later on.[xiii]

Researchers from Crowdstrike have attributed this incident to a group called "Labyrinth Chollima," which is a part of the larger "Lazarus Group," known for its North Korean directed malicious cyber activity.[xiv] 3CX Chief Information Security Officer, Pierre Jourdan, posted a blog to the company website listing the app versions affected and noted that the majority of the domains used in the hacking campaign have been taken down, mitigating the threat.[xv] Jourdan did, however, state that "...this appears to have been a targeted attack from an advanced persistent threat, perhaps even state sponsored."[xvi]

Action & Analysis

Included with Health-ISAC Membership

Congress

Tuesday, April 11th:

- No relevant hearings

Wednesday, April 12th:

- No relevant meetings

Thursday, April 13th:

- No relevant hearings

International Hearings/Meetings

- No relevant meetings

EU –

- No relevant meetings

[i] https://www.congress.gov/bill/117th-congress/house-bill/2617/text
[ii] https://www.congress.gov/bill/117th-congress/house-bill/2617/text
[iii] https://www.congress.gov/bill/117th-congress/house-bill/2617/text
[iv] https://www.federalregister.gov/documents/2023/03/30/2023-06646/cybersecurity-in-medical-devices-refuse-to-accept-policy-for-cyber-devices-and-related-systems-under
[v] https://www.federalregister.gov/documents/2023/03/30/2023-06646/cybersecurity-in-medical-devices-refuse-to-accept-policy-for-cyber-devices-and-related-systems-under
[vi] https://www.federalregister.gov/documents/2023/03/30/2023-06646/cybersecurity-in-medical-devices-refuse-to-accept-policy-for-cyber-devices-and-related-systems-under
[vii] https://www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity-medical-devices-frequently-asked-questions-faqs
[viii] https://www.congress.gov/bill/117th-congress/house-bill/2617/text
[ix] https://www.congress.gov/bill/117th-congress/house-bill/2617/text
[x] https://www.wired.com/story/solarwinds-hack-supply-chain-threats-improvements/
[xi] https://www.csoonline.com/article/3677228/supply-chain-attacks-increased-over-600-this-year-and-companies-are-falling-behind.html
[xii] https://www.3cx.com/company/
[xiii] https://cyberscoop.com/3cx-hack-supply-chain-north-korea/
[xiv] https://www.crowdstrike.com/blog/crowdstrike-detects-and-prevents-active-intrusion-campaign-targeting-3cxdesktopapp-customers/
[xv] https://www.3cx.com/blog/news/desktopapp-security-alert/
[xvi] https://cyberscoop.com/3cx-hack-supply-chain-north-korea/
[xvii] https://www.cybersecuritydive.com/news/supply-chain-cyberattacks/630179/
[xviii] https://www.csoonline.com/article/3677228/supply-chain-attacks-increased-over-600-this-year-and-companies-are-falling-behind.html

[xix] https://www.cisa.gov/sites/default/files/publications/defending_against_software_supply_chain_attacks_508_1.pdf
[xx] https://csrc.nist.gov/Projects/cyber-supply-chain-risk-management
[xxi] https://csrc.nist.gov/publications/detail/sp/800-161/rev-1/final
[xxii] https://csrc.nist.gov/publications/detail/sp/800-161/rev-1/final
[xxiii] https://niccs.cisa.gov/education-training/catalog/federal-virtual-training-environment-fedvte/cyber-supply-chain-risk
[xxiv] https://www.gsa.gov/cdnstatic/Supply-Chain-Risk-Management-(SR)-Controls-%5BCIO-IT-Security-22-120%5D-04-15-2022docx.pdf
[xxv] https://www.iso.org/standard/60905.html
[xxvi] https://cloudsecurityalliance.org/artifacts/healthcare-supply-chain-cybersecurity-risk-management/
[xxvii] https://www.cisa.gov/sites/default/files/publications/defending_against_software_supply_chain_attacks_508_1.pdf
[xxviii] https://www.whitehouse.gov/wp-content/uploads/2022/02/Capstone-Report-Biden.pdf
[xxix] https://www.csis.org/analysis/takeaways-president-bidens-supply-chain-plan-2022

Reference | References

cybersecuritydive
csis
Crowdstrike
CISA AA22-040A
federalregister
CSO Online
iso
Health-ISAC
3cx
congress
3cx
NIST-CSF
Wired
NIST-CSF
gsa
FDA
Cloud Security Alliance
CISA AA22-040A
Cyberscoop
Whitehouse

Report Source(s)

Health-ISAC

Tags

Regulatory, Hacking Healthcare, Medical Devices, FDA, Supply Chain Attack

---

For Questions and/or Comments:

Please email us at contact@h-isac.org

Conferences, Webinars, and Summits:

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

Hacking Healthcare:

Written by John Banghart, who 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.

John can be reached at jbanghart@h-isac.org and jfbanghart@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.