CY2022 Administrative Subpoena for Vulnerability Notification Year in Review

Overview

CISA leads the national effort to understand, manage, and reduce cybersecurity risks. The mission includes identifying and driving mitigation of cybersecurity vulnerabilities in the digital systems that underpin the nation's critical infrastructure. A key element of these efforts includes notifying critical infrastructure entities of vulnerabilities in their systems. However, CISA cannot always identify and notify specific owners or operators of vulnerable systems because the Electronic Communications Privacy Act generally prohibits providers of electronic communications services or remote computing services—such as internet service providers—from providing customer information to the government without legal process, such as a subpoena.

To provide a mechanism for entities to disclose this crucial identifying information to CISA, subsection (p) of Section 2209 of the Homeland Security Act of 2002 (6 U.S.C. § 659[p]) grants the director of CISA the authority to issue administrative subpoenas. This authority has enabled CISA to start obtaining the information necessary to identify owners and operators of vulnerable critical infrastructure systems so CISA can notify them of the vulnerabilities and provide them with recommended actions to mitigate those vulnerabilities.

This year in review of CISA's implementation of its administrative subpoena for vulnerability notification authority provides an overview of key data points associated with CISA's use of the authority between Jan. 1, 2022, and Dec. 31, 2022. Specifically, this summary identifies the number of subpoenas issued in Calendar Year (CY) 2022, the number of vulnerable devices apparently mitigated, and the number of entities notified and their responses.

Key Data Points

During CY2022, CISA issued 122 administrative subpoenas to identify owners or operators of 544 vulnerable devices spanning 25 unique device types. Based on responses to the administrative subpoenas, CISA successfully identified 162 owners or operators for 374 of the 544 vulnerable devices and notified them of the vulnerabilities in their systems. Of the remaining 170 vulnerable devices, CISA notified the owners or operators of 118 that were either purposely deployed as honeypots or owned or operated by entities not considered to be critical infrastructure. The remaining 52 vulnerable devices were included in 21 subpoenas for which CISA did not receive responses by the end of CY2022. In CISA's follow up from CY2021—which includes notifications based on responses received in CY2022 or re-notifications—CISA notified an additional 15 owners or operators of 49 vulnerable devices. Overall in CY2022, CISA notified 177 critical infrastructure entities regarding a total of 423 vulnerable devices.

Of the 177 critical infrastructure owners or operators notified by CISA, 109 entities did not respond to the notification, 59 entities acknowledged notification receipt, and 9 entities, who CISA notified multiple times, acknowledged receipt of some notifications but did not respond to others. CISA continues to engage—for at least six months after the initial notification—with entities that still appear to be using vulnerable devices.

Following notification of the vulnerabilities, CISA regularly conducts Shodan[1] scans to determine whether the entities appear to have mitigated their vulnerable devices. A device no longer visible in Shodan does not conclusively demonstrate the entity has mitigated the vulnerability, as there could be alternative reasons a device is no longer appearing in a Shodan scan. However, receipt of the mitigation recommendations coupled with the device no longer being visible provides evidence that the entity acted on the notification to mitigate the vulnerability. For CY2022, Shodan scans indicate a total of 116 devices of the original 423 vulnerable devices owned by critical infrastructure entities appear to have been mitigated.

[1] Shodan is a web-based search, accessible to both cyber defenders and threat actors, that can query for internet-connected assets.

Key Improvements

CISA engages repeatedly to encourage the owners and operators of vulnerable devices identified through administrative subpoenas to mitigate the vulnerabilities in their devices. CISA regional offices assumed responsibility for entity notifications in September 2022. Prior to this date, notifications were conducted by CISA headquarters personnel regardless of where the vulnerable entity was located. CISA transitioned entity notifications to the regional offices to better leverage the local knowledge and connections of regional cybersecurity personnel. This transition enables these engagements to be integrated into the broad range of outreach regional personnel conduct on an ongoing basis, increasing engagement and enhancing the effectiveness of CISA's administrative subpoena authority, with significant improvements in entity responsiveness demonstrated in CY2023.

To further improve CISA's administrative subpoena execution, CISA began development of an automated system in May 2022. The new system went live in September 2022 to streamline the process of issuing subpoenas, receiving responses, and conducting notifications to potentially vulnerable entities. The automated system functions as a records management and ticketing system enabling the CISA analysts who identified the vulnerability to see whether mitigation occurred after notification to the owner or operator. This system also enables CISA to assign notifications of vulnerabilities to members of CISA's regional cybersecurity teams in the relevant geographic area. Over the course of CY2022, these changes resulted in increased numbers of successful notifications and mitigations.