CY2021 ADMINISTRATIVE SUBPOENA FOR VULNERABILITY NOTIFICATION YEAR IN REVIEW

OVERVIEW

CISA leads the national effort to understand, manage, and reduce cybersecurity risks, including by 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 the 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, as amended (6 U.S.C. § 659(p)) grants the Director of CISA the authority to issue administrative subpoenas. This new authority enabled CISA to start obtaining the information necessary to identify the owners and operators of vulnerable critical infrastructure systems so that CISA can notify them of vulnerabilities and provide them with recommended actions to mitigate those vulnerabilities.

This year-in-review summary 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 January 1, 2021, and December 31, 2021. Specifically, this summary identifies the number of subpoenas issued in Calendar Year (CY) 2021; the number of vulnerable devices apparently mitigated; and the number of entities notified and their responses.

KEY DATA POINTS

During CY2021, CISA issued 47 administrative subpoenas to identify owners or operators of a total of 221 vulnerable devices. These 221 devices span 13 unique types of vulnerable devices. From the responses to the administrative subpoenas, CISA was able to identify 67 owners or operators for 155 out of the total 221 vulnerable devices. CISA notified all 67 of the identified owners or operators regarding the vulnerabilities in their systems. The 66 remaining vulnerable devices were covered by 11 subpoenas that were issued on December 30, 2021, but for which CISA had not yet received responses by the end of CY2021.

Following notification of the vulnerabilities, CISA regularly conducts Shodan scans to determine whether the vulnerable devices appear to have been mitigated. The fact that a device is no longer visible in Shodan does not conclusively demonstrate that the vulnerability has been mitigated, as there could be alternative reasons that a device is no longer showing up in a Shodan scan. However, receipt of the mitigation recommendations coupled with the devices no longer being visible provide evidence that the entity took action based on the notification to mitigate the vulnerability. Through follow-up Shodan scans, CISA determined that 38 of the 67 entities that were identified and notified appear to have mitigated all of their vulnerable devices; 19 entities appear not to have mitigated any of their vulnerable devices (as of publication of this report); and 10 entities appear to have mitigated some—but not all—of their vulnerable devices, leaving some of their devices still vulnerable. Taken together, Shodan scans indicate that a total of 103 devices (out of the original 155 vulnerable devices) appear to have been mitigated.

Of the 67 owners or operators that CISA notified, 22 entities did not respond to the notification, 40 entities acknowledged receipt of the notification but did not engage further with CISA, 2 entities acknowledged receipt of the notification and stated that they mitigated the vulnerability, and 1 entity denied ownership of the device.