Exploitation of Mitel MiVoice Connect SA CVE-2022-29499

rapid7.com/blog/post/2022/07/07/exploitation-of-mitel-mivoice-connect-sa-cve-2022-29499/

Caitlin Condon July 7, 2022

Last updated at Fri, 08 Jul 2022 20:21:07 GMT

In April 2022, telecommunications company Mitel published a security advisory on CVE-2022-29499, a data validation vulnerability in the Service Appliance component of MiVoice Connect, a business communications product. The vulnerability, which was unpatched at time of publication, arose from insufficient data validation for a diagnostic script and potentially allowed an unauthenticated remote attacker to send specially crafted requests to inject commands and achieve remote code execution. CVE-2022-29499 has a CVSSv3 score of 9.8.

On June 23, 2022, security firm Crowdstrike published an analysis on a ransomware intrusion attempt that had targeted CVE-2022-29499 — which at the time of detection was an undisclosed zero-day vulnerability — as an initial access vector. Over the past two weeks, Rapid7 Managed Detection and Response (MDR) has also observed a small number of intrusions that have leveraged CVE-2022-29499 as an initial access vector.

There is currently no indication that a large number of these appliances are exposed to the public internet, and we have no evidence that this vulnerability is being targeted in wider-scale ransomware campaigns. We are conscious of the fact, however, that the proliferation of ransomware in general has continued to shape risk models for many organizations, and that network perimeter devices are tempting targets for a variety of attackers.

Affected products

CVE-2022-29499 affects MiVoice Connect deployments (including earlier versions 14.2) that include the MiVoice Connect Service Appliances, SA 100, SA 400 and/or Virtual SA. Vulnerable firmware versions include R19.2 SP3 (22.20.2300.0) and earlier, and R14.x and earlier. See Mitel product security advisory 22-0002 and their security bulletin for additional information.

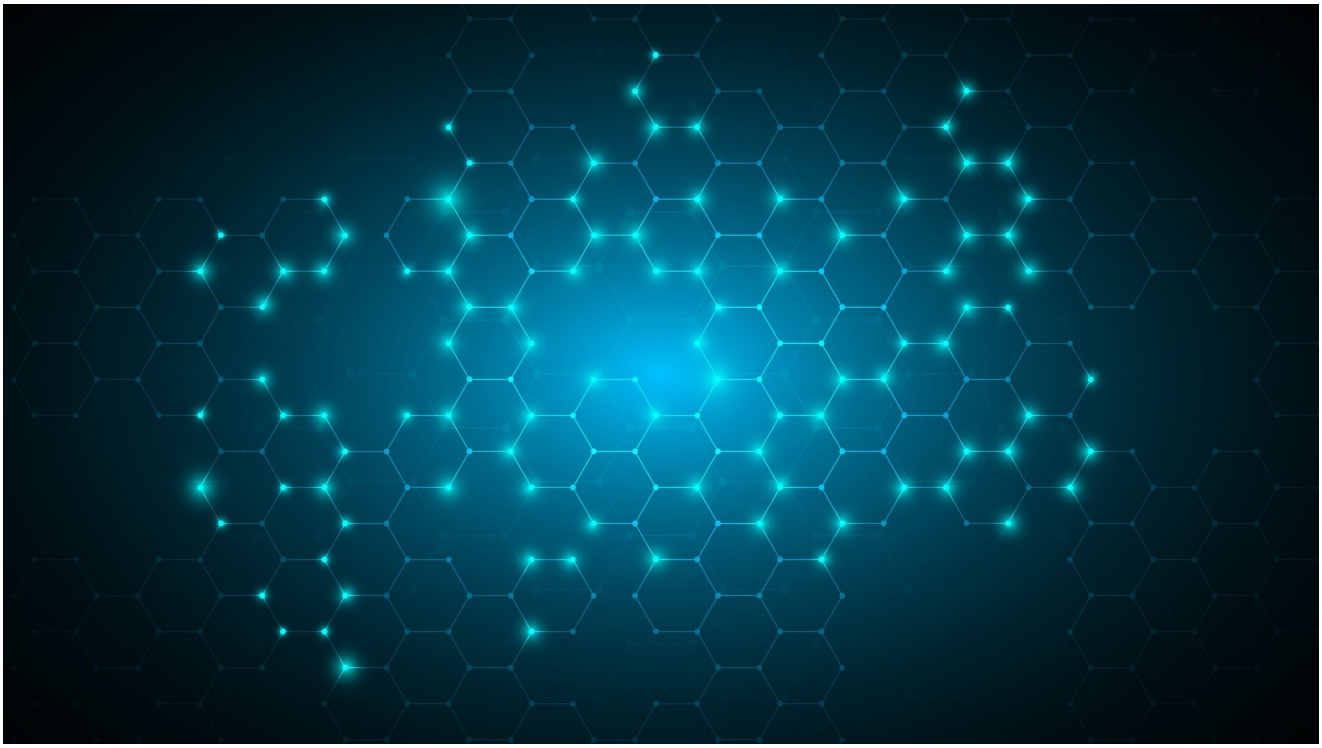
Mitigation guidance

Mitel MiVoice Connect customers who use vulnerable versions of the Service Appliance in their deployments should update to a fixed version of the appliance immediately. Mitel released patches for CVE-2022-29499 in early June 2022; organizations that have not updated the firmware on their appliances since before that timeframe should apply fixes as

soon as possible. Appliances should not be exposed to the open internet. Administrators should also review network filters for these devices and employ the principle of least privilege.

Rapid7 customers

InsightVM and Nexpose customers can assess their exposure to CVE-2022-29499 with a remote, version-based vulnerability check in the July 8, 2022 content release.



Never miss a blog

Get the latest stories, expertise, and news about security today.