aDvens

Security for the greater good

Newscast

Critical vulnerability in Google Nest

2024-01-03 | **TLP:CLEAR** | CERT aDvens - CTI

Advens - 16 Quai de la Mégisserie - 75001 Paris

Table of content

GOOGLE

Google published a security bulletin on December 11, 2023 regarding a **critical** vulnerability in Nest, its home automation synchronization tool for home networks.

Google Nest - CVE-2023-48419

Security researchers have discovered a flaw affecting Google Nest connected devices. Automatic OTA (*Over-the-Air*) updates were deployed during December 2023.

Few technical details are revealed. Exploitation of this vulnerability by an attacker located near a Google Home Wi-Fi network can spy on the victim and escalate his privileges.

Type of vulnerability

- CWE-269: Improper Privilege Management

Risks

- Privilege escalation

Criticality (CVSS v3.1 base score)

Attack vector	Network	Scope	Changed
Attack complexity	Low	Impact on confidentiality	High
Privileges Required	None	Impact on integrity	High
User Interaction	None	Impact on availability	High

Products impacted

Management firmware for the following systems or devices:

- Google Nest Audio
- Google Nest Mini
- Google Home Mini
- Google Home

Recommendations

Google has rolled out automatic updates to firmware version 2.58 for vulnerable devices during December 2023. No action is required from users.

Publisher's website

- Additional information is available in the Google Bulletin Google advisory.

Proof of concept

No proof of concept is available in open source.

Sources

GOOGLE

- https://support.google.com/product-documentation/answer/14273332?hl=en&ref_topic=12974021&sjid=4533873659772963473-NA#zippy=%2Cspeakers

CVE-2023-48419

- https://nvd.nist.gov/vuln/detail/CVE-2023-48419
- https://vuldb.com/fr/?id.249528