America's Cyber Defense Agency

NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

ICS ADVISORY

Gardyn Home Kit (Update A)

Last Revised: April 02, 2026 **Alert Code:** ICSA-26-055-03

RELATED TOPICS: INDUSTRIAL CONTROL SYSTEM VULNERABILITIES </topics/industrial-control-systems/industrial-control-system-vulnerabilities>, INDUSTRIAL CONTROL SYSTEMS </topics/industrial-control-systems>

View CSAF <https://github.com/cisagov/csaf/blob/develop/csaf_files/ot/white/2026/icsa-26-055-03.json>

Summary

Successful exploitation of these vulnerabilities could allow unauthenticated users to access and control edge devices, access cloud-based devices and user information without authentication, and pivot to other edge devices managed in the Gardyn cloud environment.

The following versions of Gardyn Home Kit (Update A) are affected:

- Gardyn Home Firmware

- Gardyn Studio Firmware
- Gardyn Mobile Application <2.11.0 (CVE-2025-1242, CVE-2025-10681)
- Gardyn Cloud API <2.12.2026 (CVE-2025-1242, CVE-2025-10681, CVE-2026-28766, CVE-2026-25197, CVE-2026-32646, CVE-2026-28767, CVE-2026-32662)

CVSS	Vendor	Equipment	Vulnerabilities
v3 9.3	Gardyn	Gardyn Home Kit (Update A)	Cleartext Transmission of Sensitive Information, Use of Default Credentials, Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection'), Use of Hard-coded Credentials, Missing Authentication for Critical Function, Authorization Bypass Through User-Controlled Key, Active Debug Code

Background

- **Critical Infrastructure Sectors:** Food and Agriculture
- **Countries/Areas Deployed:** United States
- **Company Headquarters Location:** United States

Vulnerabilities

Expand All +

CVE-2025-29628 +

CVE-2025-29629 +

CVE-2025-29631 +

CVE-2025-1242 +

CVE-2025-10681 +

CVE-2026-28766 +

CVE-2026-25197 +

CVE-2026-32646 +

CVE-2026-28767 +

CVE-2026-32662 +

Acknowledgments

- Michael Groberman reported these vulnerabilities to CISA

Legal Notice and Terms of Use

Recommended Practices

CISA recommends users take defensive measures to minimize the risk of exploitation of these vulnerabilities.

Minimize network exposure for all control system devices and/or systems, ensuring they are not accessible from the Internet.

Locate control system networks and remote devices behind firewalls and isolating them from business networks.

When remote access is required, use more secure methods, such as Virtual Private Networks (VPNs), recognizing VPNs may have vulnerabilities and should be updated to the most current version available. Also recognize VPN is only as secure as the connected devices.

CISA reminds organizations to perform proper impact analysis and risk assessment prior to deploying defensive measures.

CISA also provides a section for control systems security recommended practices on the ICS webpage on cisa.gov/ics. Several CISA products detailing cyber defense best practices are available for reading and download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.

CISA encourages organizations to implement recommended cybersecurity strategies for proactive defense of ICS assets.

Additional mitigation guidance and recommended practices are publicly available on the ICS webpage at cisa.gov/ics in the technical information paper, ICS-TIP-12-146-01B--Targeted Cyber Intrusion Detection and Mitigation Strategies.

Organizations observing suspected malicious activity should follow established internal procedures and report findings to CISA for tracking and correlation against other incidents.

No known public exploitation specifically targeting these vulnerabilities has been reported to CISA at this time.

Revision History

- **Initial Release Date:** 2026-02-24

Date	Revision	Summary
2026-02-24	1	Initial Publication

Date	Revision	Summary
2026-04-02	2	Update A - Added vulnerabilities (CVE-2025-10681, CVE-2026-28766, CVE-2026-25197, CVE-2026-32646, CVE-2026-28767, CVE-2026-32662), modified mitigations as recommended by Gardyn, associated affected products with relevant vulnerabilities, updated product version numbers.

Legal Notice and Terms of Use

Tags

Sector: Food and Agriculture Sector </topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/food-and-agriculture-sector>

Topics: Industrial Control System Vulnerabilities </topics/industrial-control-systems/industrial-control-system-vulnerabilities>, Industrial Control Systems </topics/industrial-control-systems>

Please share your thoughts

We recently updated our anonymous product survey; we welcome your feedback.

Related Advisories

APR 02, 2026 ■ ICS ADVISORY | ICSA-26-092-02

Yokogawa CENTUM VP </news-events/ics-advisories/icsa-26-092-02>

APR 02, 2026 ■ ICS ADVISORY | ICSA-26-092-01

Siemens SICAM 8 Products </news-events/ics-advisories/icsa-26-092-01>

APR 02, 2026 ■ ICS ADVISORY | ICSA-26-092-03

Hitachi Energy Ellipse </news-events/ics-advisories/icsa-26-092-03>

MAR 31, 2026 ■ ICS ADVISORY | ICSA-26-090-01

Anritsu Remote Spectrum Monitor </news-events/ics-advisories/icsa-26-090-01>

Return to top

Topics </topics> **Spotlight** </spotlight> **Resources & Tools** </resources-tools>

News & Events </news-events> **Careers** </careers> **About** </about>

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

CISA Central

1-844-Say-CISA contact@cisa.dhs.gov