The latest security information on Intel® products.

Report a Vulnerability   Product Support

Intel® RealSense™ ID Solution F450 Advisory

Intel ID:	INTEL-SA-00595
Advisory Category:	Firmware
Impact of vulnerability:	Escalation of Privilege
Severity rating:	MEDIUM
Original release:	05/10/2022

Intel ID:	INTEL-SA-00595
Last revised:	05/10/2022

Summary:

A potential security vulnerability in the Intel® RealSense™ ID Solution F450 may allow escalation of privilege. Intel is releasing firmware updates to mitigate this potential vulnerability.

Vulnerability Details:

CVEID: CVE-2021-33130

Description: Insecure default variable initialization of Intel(R) RealSense(TM) ID Solution F450 before version 2.6.0.74 may allow an unauthenticated user to potentially enable information disclosure via physical access.

CVSS Base Score: 4.8 Medium

CVSS Vector: CVSS:3.1/AV:P/AC:H/PR:N/UI:R/S:C/C:H/I:N/A:N

Affected Products:

Intel® RealSense™ ID Solution F450 before version 2.6.0.74.

Recommendations:

Intel recommends updating the Intel® RealSense™ ID Solution F450 to version 2.6.0.74 or later.

Updates are available for download at this location:
https://github.com/IntelRealSense/RealSenseID/releases/tag/v0.17.1

Acknowledgements:

The following issue was found internally by Intel employees. Intel would like to thank Julien Lenoir, Kristin Paget, Peter Bosch, John Whiteman, Nael Masalha and William Burton.

Intel, and nearly the entire technology industry, follows a disclosure practice called Coordinated Disclosure, under which a cybersecurity vulnerability is generally publicly disclosed only after mitigations are available.

Revision History

Revision	Date	Description
1.0	05/10/2022	Initial Release

Legal Notices and Disclaimers

Report a Vulnerability

If you have information about a security issue or vulnerability with an **Intel branded product or technology**, please send an e-mail to secure@intel.com   . Encrypt sensitive information using our PGP public key   .

Please provide as much information as possible, including:

- The products and versions affected
- Detailed description of the vulnerability
- Information on known exploits

A member of the Intel Product Security Team will review your e-mail and contact you to collaborate on resolving the issue. For more information on how Intel works to resolve security issues, see:

- Vulnerability handling guidelines

For issues related to Intel's external web presence (Intel.com and related subdomains), please contact Intel's External Security Research   team.

Need product support?

If you...

- Have questions about the security features of an Intel product
- Require technical support
- Want product updates or patches

Please visit Support & Downloads   .

Company Overview

Contact Intel

Newsroom

Investors

Careers

Corporate Responsibility

Diversity & Inclusion

Public Policy