

Forum:[Hack Forums](#)

Thread: [Trane Tracer SC, Tracer SC+, and Tracer Concierge](#)

Stanley - March 27, 2026, 6:20 am

Trane Tracer SC, Tracer SC+, and Tracer Concierge

View CSAF

Summary

Successful exploitation of these vulnerabilities could allow an attacker to disclose sensitive information, execute arbitrary commands, or perform a denial-of-service on the product.

The following versions of Trane Tracer SC, Tracer SC+, and Tracer Concierge are affected:

Tracer SC

Tracer SC+

Tracer Concierge

CVSS

Vendor

Equipment

Vulnerabilities

v3 8.1

Trane

Trane Tracer SC, Tracer SC+, and Tracer Concierge

Use of a Broken or Risky Cryptographic Algorithm, Memory Allocation with Excessive Size Value, Missing Authorization, Use of Hard-coded Credentials, Use of Hard-coded, Security-relevant Constants

Background

Critical Infrastructure Sectors: Critical Manufacturing

Countries/Areas Deployed: Worldwide

Company Headquarters Location: Ireland

Vulnerabilities

Expand All +

CVE-2026-28252

A Use of a Broken or Risky Cryptographic Algorithm vulnerability in Trane Tracer SC, Tracer SC+, and Tracer Concierge could allow an attacker to bypass authentication and gain root-level access to the device.

[View CVE Details](#)

Affected Products

Trane Tracer SC, Tracer SC+, and Tracer Concierge

Vendor:Trane

Product Version:Trane Tracer SC: <v4.4_SP7, Trane Tracer SC+: <v6.3.2310, Trane Tracer Concierge: <v6.3.2310

Product Status:known_affected

Remediations

Vendor fixTrane has released the following versions of Tracer SC+ for users to upgrade to:

Vendor fixCVE-2026-28252, CVE-2026-28253, CVE-2026-28254: Tracer SC+ version v6.30.2313

Relevant CWE: CWE-327 Use of a Broken or Risky Cryptographic Algorithm

Metrics

CVSS Version

Base Score

Base Severity

Vector String

3.0

8.1

HIGH

CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

CVE-2026-28253

A Memory Allocation with Excessive Size Value vulnerability in Trane Tracer SC, Tracer SC+, and Tracer Concierge could allow an unauthenticated attacker to cause a denial-of-service condition.

[View CVE Details](#)

Affected Products

Trane Tracer SC, Tracer SC+, and Tracer Concierge

Vendor:Trane

Product Version:Trane Tracer SC: <v4.4_SP7, Trane Tracer SC+: <v6.3.2310, Trane Tracer Concierge: <v6.3.2310

Product Status:known_affected

Remediations

Vendor fixTrane has released the following versions of Tracer SC+ for users to upgrade to:

Vendor fixCVE-2026-28252, CVE-2026-28253, CVE-2026-28254: Tracer SC+ version v6.30.2313

Relevant CWE: CWE-789 Memory Allocation with Excessive Size Value

Metrics

CVSS Version

Base Score

Base Severity

Vector String

3.0

7.5

HIGH

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

CVE-2026-28254

A Missing Authorization vulnerability in Trane Tracer SC, Tracer SC+, and Tracer Concierge could allow an unauthenticated attacker to access sensitive information through unprotected APIs.

[View CVE Details](#)

Affected Products

Trane Tracer SC, Tracer SC+, and Tracer Concierge

Vendor:Trane

Product Version:Trane Tracer SC: <v4.4_SP7, Trane Tracer SC+: <v6.3.2310, Trane Tracer Concierge: <v6.3.2310

Product Status:known_affected

Remediations

Vendor fixTrane has released the following versions of Tracer SC+ for users to upgrade to:
Vendor fixCVE-2026-28252, CVE-2026-28253, CVE-2026-28254: Tracer SC+ version v6.30.2313

Relevant CWE: CWE-862 Missing Authorization

Metrics

CVSS Version

Base Score

Base Severity

Vector String

3.0

5.8

MEDIUM

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:N/A:N

CVE-2026-28255

A Use of Hard-coded Credentials vulnerability in Trane Tracer SC, Tracer SC+, and Tracer Concierge could allow an attacker to disclose sensitive information and take over accounts.
[View CVE Details](#)

Affected Products

Trane Tracer SC, Tracer SC+, and Tracer Concierge

Vendor:Trane

Product Version:Trane Tracer SC: <v4.4_SP7, Trane Tracer SC+: <v6.3.2310, Trane Tracer Concierge: <v6.3.2310

Product Status:known_affected

Remediations

Vendor fixTrane has released the following versions of Tracer SC+ for users to upgrade to:
MitigationCVE-2026-28255: Trane has implemented enhanced cloud security controls to mitigate this vulnerability.

Relevant CWE: CWE-798 Use of Hard-coded Credentials

Metrics

CVSS Version
Base Score
Base Severity
Vector String

3.1
6.8
MEDIUM
CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N

CVE-2026-28256

A Use of Hard-coded, Security-relevant Constants vulnerability in Trane Tracer SC, Tracer SC+, and Tracer Concierge could allow an attacker to disclose sensitive information and take over accounts.

[View CVE Details](#)

Affected Products

Trane Tracer SC, Tracer SC+, and Tracer Concierge

Vendor:Trane

Product Version:Trane Tracer SC: <v4.4_SP7, Trane Tracer SC+: <v6.3.2310, Trane Tracer Concierge: <v6.3.2310

Product Status:known_affected

Remediations

Vendor fixTrane has released the following versions of Tracer SC+ for users to upgrade to:
MitigationCVE-2026-28256: Trane has implemented enhanced security controls which have been communicated to their customers. For more information, contact Trane.

Relevant CWE: CWE-547 Use of Hard-coded, Security-relevant Constants

Metrics

CVSS Version
Base Score

Base Severity
Vector String

3.1
5.8
MEDIUM
CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:C/C:H/I:N/A:N

Acknowledgments

Noam Moshe of Claroty reported these vulnerabilities to CISA

Legal Notice and Terms of Use

This product is provided subject to this Notification (<https://www.cisa.gov/notification>) and this Privacy & Use policy (<https://www.cisa.gov/privacy-policy>).

Recommended Practices

CISA recommends users take defensive measures to minimize the risk of exploitation of these vulnerabilities, such as:

- 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](https://www.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](https://www.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.

- CISA also recommends users take the following measures to protect themselves from social engineering attacks:

 - Do not click web links or open attachments in unsolicited email messages.

Refer to Recognizing and Avoiding Email Scams for more information on avoiding email scams.
Refer to Avoiding Social Engineering and Phishing Attacks for more information on social engineering attacks.
No known public exploitation specifically targeting these vulnerabilities has been reported to CISA at this time.

Revision History

Initial Release Date: 2026-03-12

Date	Revision	Summary
------	----------	---------

2026-03-12	1	Initial Publication
------------	---	---------------------

Legal Notice and Terms of Use

<https://www.cisa.gov/news-events/ics-advisories/icsa-26-071-01>