Vulnerability Information
Claroty SRA Privilege

Version:	1.2
Creator:	Felix Eberstaller
Reviewer:	Thomas Brandstetter
Published at:	30.06.2021
Classification:	Public

Versions

Version	Date	Comment
1.0	21.04.2021	Initial version
1.1	09.06.2021	Updated the version and timeline
1.2.	21.06.2021	Updated the version and timeline

1 VULNERABILITY INFORMATION

1.1 Summary

Vendor	Claroty
Product	Secure Remote Access Site (SRA)
Product version	SRA-3.0.1.19802d

During an OT security assessment, we found a vulnerability in the Secure Remote Access (SRA) Software of Claroty. The product Claroty SRA Site manages remote access functions for OT systems and industrial networks. The vulnerability enables an attacker with local (Linux) system access to bypass access controls for the central configuration file of the SRA Site Software. The result is access to a secret key to generate valid session tokens, which compromises the installation as it exposes the assets managed by Claroty SRA.

1.2 Risk Evaluation

CVSS Score	5.5
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N
CVE	CVE-2021-32958 (via ICSA-21-180-06)
CWE	CWE-288: Authentication Bypass Using an Alternate Path or Channel

Successful exploitation allows an attacker to gain the secret key, subsequentially allowing him to generate valid session tokens for the web UI. With access to the web UI, the attacker gets exposure to the assets managed by the SRA installation, therefore potentially compromising the installation.

1.3 Remediation / Solution

The vendor confirmed the vulnerability and provides remediation, we recommend to follow remediation suggestions.

1.4 Vendor Contact Timeline

26.01.2021	Contacting Claroty via secure@claroty.com
03.02.2021	Call with vendor. Agreed to 90 days disclosure time.
27.04.2021	Sent preliminary advisory to Claroty. Set publication date to 05.05.2021
25.05.2021	additional reachout to vendor for coordinated disclosure
09.06.2021	additional reachout to vendor for coordinated disclosure
15.06.2021	Vendor confirmation of the publication date
29.06.2021	Coordinated publication of the advisory