



TEAM82

[Research](#)[Vulnerability Dashboard](#)[Talks](#)[Tools](#)[About](#)[← Back to Dashboard](#)**HIGH THREAT**

CVE-2023-49900

X-Rite MA-T6 Kohinoor firmware, before version v2.33, is susceptible to remote code execution due to incorrectly sanitizing user input in the SetParameter command.

Risk Information

CVE ID

CVE-2023-49900

VENDOR

X-Rite

PRODUCT

Spectrophotometer

CVSS V3

8.8

[Disclosure Policy](#)

Team82 is committed to privately reporting vulnerabilities to affected vendors in a coordinated, timely manner in order to ensure the safety of the cybersecurity ecosystem worldwide. To engage with the vendor and research community, Team82 invites you to download and share our Coordinated Disclosure Policy. Team82 will adhere to this reporting and disclosure process when we discover vulnerabilities in products and services.

[Download](#) 

Public Email & PGP Key

Team82 has also made its public PGP Key available for the vendor and research community to securely and safely exchange vulnerability and research information with us.

 [See PGP Key](#)

SOLUTIONS

[Claroty xDome Platform](#)
[Industrial Cybersecurity](#)
[Healthcare Cybersecurity](#)
[Commercial Cybersecurity](#)
[Public Sector Cybersecurity](#)

PARTNERS

[Partners](#)
[Technology Alliance Partners](#)
[Channel Partners](#)

THREAT RESEARCH

[Team82 Home](#)
[Vulnerability Disclosure Dashboard](#)
[Research](#)
[PGP Key](#)

RESOURCES

[Resource Library](#)
[Blog](#)
[White Papers](#)

[Become a Partner](#)

[Partner Login](#)

[Reports](#)

[Case Studies](#)

[Datasheets](#)

[Integration Briefs](#)

[Videos](#)

[Claroty Nexus](#)

COMPANY

[About Us](#)

[Careers](#)

[Leadership](#)

[Newsroom](#)

[xCel Enablement & Training](#)

[Trust Center](#)

[Customer Experience](#)

[Events](#)

[Environmental, Social, and Governance](#)

[Policies](#)

[Contact Us](#)



© 2026 Claroty. All rights reserved.

[Terms & Conditions](#) / [Privacy Policy](#)