Compromised eMudhra CA

Date: October 29, 2026

Version : 1.0

Summary

VIAVI Solutions is aware of the recently disclosed security incident involving the eMudhra certificate authority (CA). VIAVI product teams are assessing potential impact across applicable NSE products .

The issue is not a vulnerability in VIAVI software, but may affect products or components that rely on impacted eMudhra certificates through their certificate trust stores

The assessment is ongoing. Additional information regarding product impact and recommended mitigation, if required, will be published as it becomes available. VIAVI is not currently aware of any exploitation of VIAVI products related to this vulnerability.

Vulnerability Details

The private keys of eight eMudhra (emSign) intermediate CA certificates were compromised. The keys were generated with insufficient entropy during a key ceremony in April 2025, so anyone can recover them from the public certificates. Six of the intermediates issue TLS certificates and two are code-signing CAs. An attacker holding these keys could create certificates that appear trusted, enabling impersonation, meddler-in-the-middle interception of encrypted traffic, or signing of code under any publisher name.

A researcher reported the issue on October 17, 2026. Chrome and Mozilla blocked the certificates that day, Apple followed on October 19, and Microsoft on October 20; eMudhra has since revoked them. Microsoft also removed related eMudhra roots from the Windows trust list (October 26) and the Edge trust list (October 27). No malicious use had been confirmed as of October 21, 2026. Risk is highest for non-browser clients, such as containers, build pipelines, embedded and IoT devices, and applications built on Go, Java, Node.js, or Python (certifi), that carry their own trust stores or skip revocation checks. The CA incident itself has no CVE or CVSS score; downstream fixes are tracked as CVE-2026-111943 (Go) and CVE-2026-113470 (Firefox).

References

https://www.microsoft.com/en-us/msrc/blog/2026/10/microsoft-response-to-compromised-emudhra-certificate-authority-keys

https://unit42.paloaltonetworks.com/emudhra-certificate-compromise/

https://ubuntu.com/blog/emudhra-ca-compromise-fixes-available