SHEL-2026-001

Compromised eMudhra certificate authority in the device trust store

Identifier	SHEL-2026-001
Severity	Critical (9.5, CVSS 4.0) CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:L
CVE	None assigned
Affected products	Shelly Gen2 and newer devices, including Shelly BLU Gateway and Shelly cameras, on firmware without the fix
Fixed in	1.7.6, 2.0.3 and 2.1.1 (stable); 2.2.0-beta2 (beta); 2.3.99-cameraprod13 (Shelly cameras)
Published	2026-11-09
Last updated	2026-11-17
Advisory version	1.1

1. Summary

Shelly devices check the TLS certificate of each server they connect to against a list of trusted root certificates built into the firmware. Older firmware trusted two root certificates under which eight eMudhra intermediate certificate authorities were issued. The private keys of those intermediates could be recovered, so they must be treated as compromised.

Firmware 1.7.6, 2.0.3 and 2.1.1, and 2.3.99-cameraprod13 for Shelly cameras, remove these roots from the device trust store. We recommend that all users update their devices.

2. Background

On 17 October 2026, Mozilla received a report that the private keys of eight eMudhra intermediate certificate authorities, six for TLS and two for code signing, had been compromised. eMudhra revoked all eight on 18 October 2026 and describes the cause as cryptographically weak keys. Mozilla published its response on 20 October 2026 and has removed the root "emSign ECC Root CA - G3" from its trusted root list.

Browsers are protected through their own update and revocation mechanisms. Shelly devices rely only on the trust store built into their firmware, so the affected roots had to be removed with a firmware update.

The roots removed are "AAA Certificate Services" (Sectigo, formerly Comodo) and "emSign ECC Root CA - G3" (eMudhra). The update also brings the full trust store in line with the current Mozilla root list, which removes further roots that Mozilla no longer trusts.

3. Impact

Anyone holding one of the compromised keys can create a certificate for any domain name, and a device on older firmware would accept it as valid. An attacker who can also intercept the device's network traffic, for example through a compromised router, a rogue Wi-Fi network or DNS hijacking, could impersonate any HTTPS, MQTT or WebSocket server that the device checks against its built-in trust store. This includes the Shelly cloud connection, MQTT brokers set up by the user and servers called by user scripts.

Such an attacker could read credentials and tokens that the device sends, and forge commands or responses, for example to switch outputs, change the configuration or alter what a script does.

Connections for which the user uploaded their own CA certificate do not use the built-in trust store and are not affected.

4. Affected products and fixed versions

Shelly Gen2 and newer devices (Plus, Pro, Gen3 and Gen4), including Shelly BLU Gateway and Shelly cameras, on the firmware versions below.

Firmware line	Affected versions	Fixed version
1.x	Earlier than 1.7.6	1.7.6
2.0	2.0.x earlier than 2.0.3	2.0.3
2.1	2.1.x earlier than 2.1.1	2.1.1
2.2 (beta)	2.2.0-beta1	2.2.0-beta2
Shelly cameras	Earlier than 2.3.99-cameraprod13	2.3.99-cameraprod13

Devices that have not received the 2.0 firmware line can update to 1.7.6.

This advisory covers Gen2 and newer devices.

Shelly BLU Gateway gets the fix in 1.7.6. Shelly BLU Gateway Gen3 gets it in 2.0.3 (stable) and 2.2.0-beta2 (beta).

Shelly Wall Display runs separate firmware and is being checked. This advisory will be updated with the result.

5. What you should do

- Update your devices to the fixed firmware for their line, in the Shelly Smart Control app or in the device's local web interface.
- For MQTT and outbound WebSocket connections, use your own CA certificate instead of the built-in trust store.
- Keep the network path secure, for example by keeping your router firmware up to date. If a device cannot be updated yet, keep it on a network you trust.
- Check your devices for scripts, webhooks, schedules or configuration changes that you did not make.

6. Exploitation

Shelly is not aware of this issue being exploited against Shelly devices.

7. Acknowledgements

Shelly thanks a member of the Shelly community for reporting this issue.

8. References

- Mozilla bug 2083449: eMudhra: Private key compromise of Intermediate Certificates: https://bugzilla.mozilla.org/show_bug.cgi?id=2083449
- Mozilla Security Blog, 20 October 2026: https://blog.mozilla.org/security/2026/10/20/protecting-firefox-users-following-the-compromise-of-emudhra-intermediate-certificates/

- eMudhra statement on the certificate security incident: https://emudhra.com/en/post/certificate-security-incident
- Red Hat RHSB-2026-012, eMudhra certificate compromise: https://access.redhat.com/security/vulnerabilities/RHSB-2026-012

9. Contact

To report a security issue in a Shelly product or service, write to security@shelly.com. Our Vulnerability Disclosure Policy and report form are at https://security.shelly.com. The latest version of this advisory is listed at https://security.shelly.com/advisories/.

10. Revision history

Version	Date	Change
1.0	2026-11-09	Initial publication
1.1	2026-11-17	Moved to security.shelly.com; links updated. No change to the technical content.

11. Disclaimer

This advisory is provided “as is” as of the date of publication and may be updated as new information becomes available.