CHeKT Security Bulletin

November 2026. For CHeKT partners, dealers, monitoring centers and their customers.

Dear CHeKT Partners,

This notice is to provide details regarding a couple of global cybersecurity incidents that occurred during the month of October. The CHeKT cloud DevOps team was tracking these incidents as they were reported in the market and has responded accordingly based on how the announced vulnerabilities affected technology platforms.

CHeKT solution and products were not affected by the PHP vulnerabilities disclosed in October, and no action was needed to reduce any risk of exposure for customers, security providers or monitoring center customers. CHeKT's public marketing website, www.chekt.com, does use PHP. It holds no customer data, and it was patched within 24 hours with no evidence of exploitation.

A cyber risk related to certificate authorities was also announced in October, and it came from a flawed key generation process at one certificate authority. In order to remove any risk to CHeKT customers, CHeKT has released Bridge firmware 6.3.0. This update closes any risk created by the industry wide certificate authority issue.

We recommend that every dealer update all CHeKT Bridges to firmware 6.3.0 as soon as possible.

Over the past few weeks, many of you have asked how these two industry events affect CHeKT. This bulletin answers those questions in one place, in plain terms, so you can share it with your customers and monitoring centers. We will update it if anything changes.

Thank you for your partnership and for taking security as seriously as we do.

David Erickson
VP of Operations, CHeKT Visual Security

At a Glance

Only one of the two issues needs action from dealers: updating CHeKT Bridges to firmware 6.3.0.

Issue	Disclosed	Is CHeKT affected?	What dealers need to do
Weak certificate authority keys at eMudhra (emSign), cross signed by Sectigo	17 October 2026	The CHeKT Bridge trusted the affected certificate authorities. No CHeKT system was compromised and no misuse has been found. Fixed in firmware 6.3.0.	Update every CHeKT Bridge to firmware 6.3.0
PHP vulnerabilities: CVE-2026-109618 CVE-2026-109619 CVE-2026-115560	21 and 23 October 2026	No. CHeKT products and services do not use PHP.	Nothing

Industry Certificate Authority Issue: Update to Firmware 6.3.0

Firmware 6.3.0 is a preventive security update. No CHeKT system was compromised, and CHeKT has found no evidence that this issue was used against any CHeKT Bridge, customer or monitoring center.

What Happened

On 17 October 2026, researchers reported that eight intermediate certificate authority keys created by eMudhra, the company behind the emSign brand, were so weak that anyone could calculate them from public information. Sectigo had also cross signed the same keys under its widely trusted AAA Certificate Services root.

In lay terms, anyone holding these keys could create a convincing fake security certificate for almost any website or server. eMudhra and Sectigo revoked the affected certificates, and Chrome, Firefox and Apple blocked them within days.

What It Means for the CHeKT Bridge

Web browsers received those blocks automatically. Connected devices that carry their own list of trusted certificate authorities did not, and the CHeKT Bridge is one of them.

Every publicly released CHeKT Bridge firmware version before 6.3.0 trusted AAA Certificate Services and four emSign root certificates. In theory, someone who could intercept a specific Bridge's internet connection could have used a fake certificate to impersonate the CHeKT cloud to that Bridge. While there is no current evidence of any breach, if this were to happen, the risk would be isolated to that specific Bridge and its associated cameras.

What CHeKT Has Done

- **Firmware 6.3.0 blocks all five affected root certificates** on the CHeKT Bridge: AAA Certificate Services, emSign Root CA G1, emSign ECC Root CA G3, emSign Root CA C1 and emSign ECC Root CA C3. CHeKT's cloud services never relied on these certificate authorities, so Bridges keep connecting normally after the update.

- **CHeKT verified the block against Mozilla's public test servers.** Bridges running the 6.3.0 build rejected the affected certificates through both the emSign path and the Sectigo cross signed path, on current and older Bridge operating systems. Connections to servers using current Sectigo (USERTrust) certificates are not affected.
- **A new Trust Store Manager checks the Bridge every day** and keeps the affected certificates blocked if anything tries to change them.
- **CHeKT updated its cloud services**, starting with the highest priority services, and is completing the remaining services in phases.
- **CHeKT coordinated its response with the Alarm.com security team.**
- **Next, CHeKT is designing a way to manage the Bridge's trusted certificate list from the cloud** and deliver changes securely, so future industry issues can be handled faster. This is a future enhancement and is not part of 6.3.0.

What Dealers Need to Do

1. Update every CHeKT Bridge to firmware 6.3.0 from the CHeKT Dealer Management Portal. CHeKT never updates Bridge firmware automatically, so the protection reaches a site only when its Bridge is updated.
2. To update many sites at once, use Dealer Reports in the portal.
3. Follow the step by step guide: Updating Bridge Firmware.

Cameras, NVRs and IP speakers on the site network are not affected. Bridge HTTP request (webhook) actions to outside servers keep working unless that server's certificate chains only to one of the five blocked roots.

During field testing, a small number of sites received this same build labeled 6.2.1. It carries the same certificate protection, and those sites can move to 6.3.0 with their next update. For everything else included in 6.3.0, see the 6.3.0 release notes.

PHP Vulnerabilities: CHeKT Is Not Affected

No CHeKT product or service used by dealers, customers or monitoring centers is affected, and no action is required.

On 21 October 2026, two vulnerabilities in PHP, CVE-2026-109618 and CVE-2026-109619, were publicly disclosed. CHeKT reviewed its exposure the same day, in coordination with the Alarm.com security team, and found no evidence of exploitation.

The CHeKT platform does not use PHP. That includes the CHeKT Bridge (all models and firmware versions), the CHeKT cloud, the Dealer Management Portal, the monitoring portal and the CHeKT mobile apps.

The only systems in scope were CHeKT's public marketing and content websites, such as www.chekt.com, which hold no customer data. They were patched or mitigated within the day.

CHeKT also reviewed CVE-2026-115560, reported on 23 October 2026. The recommended mitigations were already in place on our marketing website, and no evidence of exploitation was found.

These PHP vulnerabilities are unrelated to the certificate authority issue above. No firmware update is needed for them.

Questions and Contacts

For questions about this bulletin, contact your CHeKT sales representative or CHeKT Technical Support:

- Email: support@chekt.com
- Phone: +1 224 442 4358, option 1
- Toll free (US and Canada): 844 844 7685, option 1

References

- Cloudflare warns fixing botched eMudhra certs goes beyond browsers, iTnews, 21 October 2026
- About the compromised eMudhra intermediate CAs, Apple Support, 29 October 2026

***NOTE**: This bulletin reflects CHeKT's assessment as of the date above and is provided for informational purposes only. It does not constitute a contract, warranty, representation, or guarantee of any kind regarding the security of CHeKT's platform, services, or customer data.*

This document does not supersede or modify any agreement between CHeKT and any customer or partner. Customers and partners should refer to their applicable agreements with CHeKT for any contractual commitments regarding security or data privacy.