



Advisory NCSC-2026-0427

PRIORITEIT: NORMAAL

Kwetsbaarheden verholpen in Ahsay AhsayCBS

Publicatiedatum: 14-10-2026

Toegestane verspreiding: TLP:WHITE
(Traffic Light Protocol)

Deze publicatie bevat het label TLP:WHITE en wordt door het Nationaal Cyber Security Center (NCSC) verspreid. Het NCSC gebruikt het Traffic Light Protocol (TLP) om eenduidig te definiëren wat er met de informatie mag gebeuren. Wanneer informatie is voorzien van een TLP-aanduiding weet u met wie u deze informatie mag delen. Dit staat beschreven in de standaard First (www.first.org/tlp).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Reacties zijn welkom op info@ncsc.nl.

Feiten

Ahsay heeft kwetsbaarheden verholpen in AhsayCBS tot en met versie 10.3.2.

Duiding

De kwetsbaarheid met kenmerk CVE-2026-105133 heeft een CVSS-score van 7,3 en betreft onvoldoende authenticatie in de functie checkSysPwd van de AhsayCBS API. Een niet-geauthenticeerde kwaadwillende kan de kwetsbaarheid op afstand misbruiken om de authenticatie te omzeilen.

De kwetsbaarheid met kenmerk CVE-2026-105134 heeft een CVSS-score van 10,0 en betreft OS-command-injectie in de Replication Receiver via /rps/api/json/UpdateReceivers.do. De kwetsbaarheid kan op afstand worden misbruikt voor het uitvoeren van willekeurige OS-commando's.

Onderzoekers hebben actief misbruik waargenomen waarbij beide kwetsbaarheden in één aanvalsketen worden gecombineerd. Hierbij wordt CVE-2026-105133 gebruikt om de authenticatie te omzeilen, waarna CVE-2026-105134 wordt misbruikt. Hierdoor kan een niet-geauthenticeerde kwaadwillende op afstand code uitvoeren op een kwetsbare AhsayCBS-server.

Het NCSC adviseert om de beveiligingsupdates met spoed toe te passen en onderzoek te doen naar mogelijke eerdere compromittering van kwetsbare systemen. Ahsay noemt onder meer verdachte mappen en bestanden, ongeautoriseerde RPS receivers en ongeautoriseerde AhsayCBS-accounts met administratieve rechten als indicatoren. Wanneer aanwijzingen voor compromittering worden aangetroffen, adviseert Ahsay de server volledig opnieuw op te bouwen en een configuratie van vóór de compromittering te herstellen.

Zie bijgevoegde referenties voor meer informatie.

Oplossingen

Ahsay heeft versie 10.3.4 van AhsayCBS uitgebracht om deze kwetsbaarheden te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- <https://www.ahsay.com/en/company/announcements/ahsaycbs-vulnerability-status-update>
- <https://www.ahsay.com/en/company/announcements/patch-cve-105133-105134-update>

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-105134	9.3 CRITICAL
CVE-2026-105133	5.5 MEDIUM

CWE's

CWE	Beschrijving
CWE-77	Improper Neutralization of Special Elements used in a Command ('Command Injection')
CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

Getroffen producten

Ahsay
AhsayCBS

Disclaimer

The Netherlands Cyber Security Center (henceforth: NCSC-NL) maintains this page to enhance access to its information and security advisories. The use of this security advisory is subject to the following terms and conditions:

NCSC-NL makes every reasonable effort to ensure that the content of this page is kept up to date, and that it is accurate and complete. Nevertheless, NCSC-NL cannot entirely rule out the possibility of errors, and therefore cannot give any warranty in respect of its completeness, accuracy or continuous keeping up-to-date. The information contained in this security advisory is intended solely for the purpose of providing general information to professional users. No rights can be derived from the information provided therein. NCSC-NL and the Kingdom of the Netherlands assume no legal liability or responsibility for any damage resulting from either the use or inability of use of this security advisory. This includes damage resulting from the inaccuracy or incompleteness of the information contained in the advisory. This security advisory is subject to Dutch law. All disputes related to or arising from the use of this advisory will be submitted to the competent court in The Hague. This choice of means also applies to the court in summary proceedings.