Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0040

Kwetsbaarheid verholpen in SmarterTools SmarterMail

NCSC Advisory

PRIORITEIT: HOOG

Gepubliceerd op: 27-01-2026

TLP:WHITE

Toegestane verspreiding van TLP:WHITE
(Traffic Light Protocol)

Deze handreiking bevat het label TLP:WHITE en wordt door het 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.

Uw reacties zijn welkom op info@ncsc.nl

Feiten

SmarterTools heeft kwetsbaarheden verholpen in SmarterMail.

Duiding

Een kwaadwillende kan de kwetsbaarheden misbruiken om authenticatie te omzeilen en willekeurige code uit te voeren met rechten van de beheerder, en mogelijk SYSTEM.

Voor succesvol misbruik moet de kwaadwillende toegang hebben tot de API-interface (met name de `/api/v1/auth/force-reset-password` endpoint) en kan op die manier zonder voorafgaande authenticatie het wachtwoord van een beheerder resetten door middel van een speciaal geprepareerd HTTP-verzoek. Ook kan een kwaadwillende een malafide HTTP-server inrichten, om daarmee een slachtoffer te misleiden deze te bezoeken en zo willekeurige code uit te voeren op de kwetsbare server.

Voor de kwetsbaarheid met kenmerk CVE-2026-23760 is Proof-of-Concept-code gepubliceerd en het Amerikaanse CISA heeft de kwetsbaarheid op de Known Exploited Vulnerabilities-lijst geplaatst, wat aangeeft dat de kwetsbaarheid actief is misbruikt.

Oplossingen

SmarterTools heeft updates uitgebracht om de kwetsbaarheden te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Het NCSC adviseert onderzoek te doen naar de SmarterMail-omgeving en met name te controleren of van beheerdersaccounts recentelijk het wachtwoord is gewijzigd.

Referenties

- https://www.smartertools.com/smartermail/release-notes/current

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-23760	9.3 CRITICAL
CVE-2026-24423	9.3 CRITICAL

CWE's

CWE	Beschrijving
CWE-288	Authentication Bypass Using an Alternate Path or Channel
CWE-306	Missing Authentication for Critical Function

Getroffen producten

SmarterTools
SmarterMail

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 of 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.