



Advisory NCSC-2026-0408

PRIORITEIT: NORMAAL

Kwetsbaarheden verholpen in Kiteworks

Publicatiedatum: 08-10-2026

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

Kiteworks heeft meerdere kwetsbaarheden verholpen in de Kiteworks productlijn.

Duiding

De kwetsbaarheden in Kiteworks betreffen diverse componenten en functionaliteiten binnen de producten.

- Geauthenticeerde beheerders kunnen onder andere misbruik maken van onvoldoende validatie in import- en exportfuncties, wat leidt tot het schrijven van bestanden op willekeurige locaties en het uitvoeren van arbitrary code.
- Er zijn meerdere gevallen van privilege-escalatie waarbij gebruikers met beperkte rechten hun privileges kunnen verhogen tot systeembeheerder.
- Verder zijn er kwetsbaarheden die het mogelijk maken om via Server-Side Request Forgery (SSRF) ongeautoriseerde verzoeken naar interne netwerken te sturen, wat toegang tot beschermde interne bronnen kan geven.
- Cross-site scripting (XSS) kwetsbaarheden maken het mogelijk om kwaadaardige scripts uit te voeren in de context van andere gebruikers, wat sessieovername kan veroorzaken.
- SQL-injectieproblemen in administratieve functies kunnen leiden tot ongeautoriseerde toegang tot databasegegevens.
- Daarnaast zijn er kwetsbaarheden in authenticatiemechanismen, waaronder bypasses en het resetten van wachtwoorden zonder juiste verificatie, wat ongeautoriseerde accounttoegang mogelijk maakt.
- Sommige kwetsbaarheden betreffen ook de cluster- en appliance-omgevingen, waarbij command execution en privilege-escalatie tussen nodes mogelijk is.
- Verder zijn er problemen met onvoldoende validatie van uploads, configuratiebestanden en certificaattoewijzingen, wat kan leiden tot systeemcompromittering of het onderscheppen van versleutelde communicatie.
- Ten slotte zijn er kwetsbaarheden die resource exhaustion kunnen veroorzaken, wat de beschikbaarheid van de systemen kan beïnvloeden.

Exploitatie van deze kwetsbaarheden vereist in veel gevallen authenticatie met beheerdersrechten, maar er zijn ook kwetsbaarheden die zonder authenticatie kunnen worden misbruikt, met name tijdens de initiële setup of via onbeveiligde interfaces. Omdat kwetsbaarheden die zonder voorafgaande authenticatie kunnen worden misbruikt mogelijk kunnen leiden tot verhoogde rechten, is het niet uitgesloten dat de kwetsbaarheden in keten kunnen worden misbruikt en kunnen leiden tot uitvoer van handelingen onder beheerdersrechten.

Oplossingen

Kiteworks heeft updates uitgebracht om de kwetsbaarheden in de Kiteworks productlijn te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- <https://github.com/kiteworks/security-advisories/security/advisories/>

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-102089	7.2 HIGH
CVE-2026-102090	4.3 MEDIUM
CVE-2026-102091	7.5 HIGH
CVE-2026-102092	8.7 HIGH
CVE-2026-102093	7.2 HIGH
CVE-2026-102094	7.2 HIGH
CVE-2026-102095	9.1 CRITICAL
CVE-2026-102096	7.2 HIGH
CVE-2026-102097	7.2 HIGH
CVE-2026-102098	7.2 HIGH
CVE-2026-102099	7.2 HIGH
CVE-2026-102100	8.7 HIGH
CVE-2026-102101	8.1 HIGH
CVE-2026-102102	9.1 CRITICAL
CVE-2026-102103	9.1 CRITICAL
CVE-2026-102104	9.1 CRITICAL
CVE-2026-102105	9.1 CRITICAL
CVE-2026-102106	9.1 CRITICAL

CVE	CVSS Score
CVE-2026-102107	4.6 MEDIUM
CVE-2026-102108	7.2 HIGH
CVE-2026-102109	7.1 HIGH
CVE-2026-102110	5.9 MEDIUM
CVE-2026-102111	4.9 MEDIUM
CVE-2026-102112	7.8 HIGH
CVE-2026-102113	7.8 HIGH
CVE-2026-102114	7.2 HIGH
CVE-2026-102115	9.8 CRITICAL
CVE-2026-102116	7.2 HIGH
CVE-2026-102117	7.2 HIGH
CVE-2026-102118	7.8 HIGH
CVE-2026-102119	7.2 HIGH
CVE-2026-102120	8.8 HIGH
CVE-2026-102121	8.6 HIGH
CVE-2026-102122	4.3 MEDIUM
CVE-2026-102123	7.4 HIGH
CVE-2026-102124	6.5 MEDIUM
CVE-2026-102125	8.8 HIGH
CVE-2026-102126	8.1 HIGH
CVE-2026-102127	7.0 HIGH
CVE-2026-102128	7.5 HIGH
CVE-2026-102129	7.2 HIGH
CVE-2026-102130	7.2 HIGH
CVE-2026-102131	7.2 HIGH
CVE-2026-102132	7.2 HIGH
CVE-2026-102133	6.6 MEDIUM
CVE-2026-102134	5.4 MEDIUM
CVE-2026-102135	6.6 MEDIUM
CVE-2026-102136	6.3 MEDIUM
CVE-2026-102137	4.1 MEDIUM

CVE	CVSS Score
CVE-2026-102138	3.3 LOW
CVE-2026-102139	6.5 MEDIUM
CVE-2026-102140	4.9 MEDIUM
CVE-2026-102141	6.7 MEDIUM
CVE-2026-102142	7.2 HIGH
CVE-2026-102143	7.5 HIGH
CVE-2026-102144	5.3 MEDIUM
CVE-2026-102145	6.6 MEDIUM
CVE-2026-102146	6.5 MEDIUM
CVE-2026-102147	9.3 CRITICAL
CVE-2026-102149	9.4 CRITICAL
CVE-2026-102150	7.2 HIGH

CWE's

CWE	Beschrijving
CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
CWE-59	Improper Link Resolution Before File Access ('Link Following')
CWE-73	External Control of File Name or Path
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')
CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
CWE-91	XML Injection (aka Blind XPath Injection)
CWE-93	Improper Neutralization of CRLF Sequences ('CRLF Injection')
CWE-94	Improper Control of Generation of Code ('Code Injection')

CWE	Beschrijving
CWE-178	Improper Handling of Case Sensitivity
CWE-250	Execution with Unnecessary Privileges
CWE-266	Incorrect Privilege Assignment
CWE-306	Missing Authentication for Critical Function
CWE-420	Unprotected Alternate Channel
CWE-434	Unrestricted Upload of File with Dangerous Type
CWE-470	Use of Externally-Controlled Input to Select Classes or Code ('Unsafe Reflection')
CWE-502	Deserialization of Untrusted Data
CWE-601	URL Redirection to Untrusted Site ('Open Redirect')
CWE-611	Improper Restriction of XML External Entity Reference
CWE-639	Authorization Bypass Through User-Controlled Key
CWE-640	Weak Password Recovery Mechanism for Forgotten Password
CWE-653	Improper Isolation or Compartmentalization
CWE-670	Always-Incorrect Control Flow Implementation
CWE-807	Reliance on Untrusted Inputs in a Security Decision
CWE-863	Incorrect Authorization
CWE-918	Server-Side Request Forgery (SSRF)
CWE-940	Improper Verification of Source of a Communication Channel
CWE-1284	Improper Validation of Specified Quantity in Input
CWE-1336	Improper Neutralization of Special Elements Used in a Template Engine

Getroffen producten

Kiteworks
Core
Email Protection Gateway
Kiteworks
Secure Data Forms

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.