Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0332

Kwetsbaarheden verholpen in Apache CloudStack

NCSC Security Advisory
Prioriteit: Normaal
Gepubliceerd op: 27-08-2026

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

Apache heeft meerdere kwetsbaarheden verholpen in Apache CloudStack, specifiek in versies 4.12.0.0 tot en met 4.22.1.0.

Duiding

De kwetsbaarheden betreffen onder andere OS Command Injection in de NAS backup provider plugin, Server-Side Request Forgery (SSRF) in verschillende modules zoals metalink mirror URL resolutie en webhook, onvoldoende toegangscontrole in userdata-gerelateerde API's, OAuth en LDAP authenticatie plugins, en improper privilege management in de two-factor authentication plugin.

Verder zijn er kwetsbaarheden in de user interface met betrekking tot onjuiste encoding of escaping, command injection in diagnostics APIs, en improper access control in Kubernetes Service plugin en annotation APIs. Ook is er een kwetsbaarheid in de SAML certificaatvalidatie die het mogelijk maakt om authenticatie te omzeilen.

Sommige kwetsbaarheden maken het mogelijk voor geauthenticeerde gebruikers om root- of administratieve commando's uit te voeren op KVM hypervisor hosts, systeem virtual machines en virtual routers, of om ongeautoriseerde toegang te verkrijgen tot gevoelige informatie en tenant data. Daarnaast is er een kwetsbaarheid in de listHostTags API die domeinrestricties kan omzeilen, en een issue in projectrollenbeheer door domeinbeheerders.

De kwetsbaarheden zijn aanwezig in meerdere opeenvolgende versies van Apache CloudStack en betreffen zowel core functionaliteiten als plugins en API's.

Oplossingen

Apache heeft updates uitgebracht in versies 4.20.3.1 en 4.22.1.1 of later om de genoemde kwetsbaarheden te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://cloudstack.apache.org/blog/security-release-advisory-4.20.3.1-4.22.1.1

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-47359	8.8 HIGH

CVE-2026-50112	8.8 HIGH
CVE-2026-50222	7.5 HIGH
CVE-2026-59085	9.1 CRITICAL
CVE-2026-59655	7.5 HIGH
CVE-2026-59657	7.5 HIGH
CVE-2026-59780	7.5 HIGH
CVE-2026-59799	8.8 HIGH
CVE-2026-61397	7.5 HIGH
CVE-2026-61398	9.1 CRITICAL
CVE-2026-61399	4.8 MEDIUM
CVE-2026-61400	8.8 HIGH
CVE-2026-61422	4.3 MEDIUM
CVE-2026-62440	9.1 CRITICAL
CVE-2026-65613	4.3 MEDIUM
CVE-2026-66721	2.7 LOW
CVE-2026-66722	7.2 HIGH
CVE-2026-66797	8.5 HIGH
CVE-2026-68745	8.1 HIGH

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')

CWE-116	Improper Encoding or Escaping of Output
CWE-172	Encoding Error
CWE-295	Improper Certificate Validation
CWE-306	Missing Authentication for Critical Function
CWE-312	Cleartext Storage of Sensitive Information
CWE-347	Improper Verification of Cryptographic Signature
CWE-862	Missing Authorization
CWE-918	Server-Side Request Forgery (SSRF)

Getroffen producten

Apache Software Foundation
CloudStack

Disclaimer