Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Advisory NCSC-2026-0519

PRIORITEIT: NORMAAL

Kwetsbaarheden verholpen in Tanium producten

Publicatiedatum: 26-11-2026

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 de-len. 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

Tanium heeft meerdere kwetsbaarheden verholpen in verschillende componenten van haar product suite, waaronder Comply, Connect, Threat Response, Core Content, Default Content, Emerging Issues Content, Engage, Enforce Recovery Key Portal, Tanium Server, Tanium Zone Server en Partner Integration.

Duiding

De kwetsbaarheden betreffen onder andere command injection, unauthorized code execution, improper input validation, argument injection, path traversal, information disclosure, local privilege escalation, denial of service en server-side request forgery (SSRF).

Aanvallers kunnen deze kwetsbaarheden misbruiken om onder meer arbitrary commands of code uit te voeren, ongeautoriseerde toegang te verkrijgen tot gevoelige data, privileges te escaleren, systeembronnen uit te putten waardoor de beschikbaarheid wordt verstoord, en ongewenste server requests te initiëren.

Oplossingen

Tanium heeft updates en patches uitgebracht om de kwetsbaarheden te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://security.tanium.com/TAN-2026-126
- https://security.tanium.com/TAN-2026-127
- https://security.tanium.com/TAN-2026-128
- https://security.tanium.com/TAN-2026-129
- https://security.tanium.com/TAN-2026-130
- https://security.tanium.com/TAN-2026-131
- https://security.tanium.com/TAN-2026-132
- https://security.tanium.com/TAN-2026-133
- https://security.tanium.com/TAN-2026-134
- https://security.tanium.com/TAN-2026-135
- https://security.tanium.com/TAN-2026-136
- https://security.tanium.com/TAN-2026-137
- https://security.tanium.com/TAN-2026-138

- https://security.tanium.com/TAN-2026-139
- https://security.tanium.com/TAN-2026-140
- https://security.tanium.com/TAN-2026-141
- https://security.tanium.com/TAN-2026-142
- https://security.tanium.com/TAN-2026-143
- https://security.tanium.com/TAN-2026-144
- https://security.tanium.com/TAN-2026-145
- https://security.tanium.com/TAN-2026-146
- https://security.tanium.com/TAN-2026-147
- https://security.tanium.com/TAN-2026-148
- https://security.tanium.com/TAN-2026-149
- https://security.tanium.com/TAN-2026-150
- https://security.tanium.com/TAN-2026-151

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-120747	8.8 HIGH
CVE-2026-131650	6.5 MEDIUM
CVE-2026-131696	3.3 LOW
CVE-2026-133863	8.8 HIGH
CVE-2026-133864	8.8 HIGH
CVE-2026-133877	6.6 MEDIUM
CVE-2026-133880	8.8 HIGH
CVE-2026-133955	7.1 HIGH
CVE-2026-133959	8.8 HIGH
CVE-2026-133960	8.8 HIGH
CVE-2026-133961	7.2 HIGH
CVE-2026-134178	4.2 MEDIUM
CVE-2026-134346	5.5 MEDIUM
CVE-2026-134443	5.3 MEDIUM

CVE	CVSS Score
CVE-2026-134493	7.5 HIGH
CVE-2026-134494	8.0 HIGH
CVE-2026-134496	7.3 HIGH
CVE-2026-134618	7.3 HIGH
CVE-2026-134619	7.3 HIGH
CVE-2026-134620	8.8 HIGH
CVE-2026-134739	6.5 MEDIUM
CVE-2026-134740	5.9 MEDIUM
CVE-2026-134746	2.4 LOW
CVE-2026-135121	5.0 MEDIUM

CWE's

CWE	Beschrijving
CWE-23	Relative Path Traversal
CWE-78	Improper Neutralization of Special Elements used in an OS Command
CWE-88	Improper Neutralization of Argument Delimiters in a Command
CWE-95	Improper Neutralization of Directives in Dynamically Evaluated Code
CWE-226	Sensitive Information in Resource Not Removed Before Reuse
CWE-306	Missing Authentication for Critical Functionality
CWE-348	Use of Less Trusted Source
CWE-354	Improper Validation of Integrity Check Value
CWE-401	Missing Release of Memory after Effective Lifetime
CWE-426	Untrusted Search Path
CWE-522	Insufficiently Protected Credentials
CWE-532	Insertion of Sensitive Information into Log File
CWE-789	Memory Allocation with Excessive Size Value
CWE-862	Missing Authorization
CWE-918	Server-Side Request Forgery

Getroffen producten

Tanium
Comply
Connect
Core Content
Emerging Issues Content
Endpoint Configuration Toolset Solution
Endpoint Management
Enforce Recovery Key Portal
Engage
Partner Integration
Tanium Module Server
Tanium Server
Tanium Zone Server
Threat Response

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.