National Cyber Security Centre

2408140167-NCSC

Department of the Environment, Climate & Communications

NCSC Alert

Critical Vulnerability exists in Ivanti Virtual Traffic Manager (vTM) (CVE-2024-7593 - CVSS3.0: 9.8)

Wednesday 14th August, 2024

STATUS: TLP-CLEAR

Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP-CLEAR *when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules,* TLP-CLEAR *information may be shared without restriction.*
For more information on the Traffic Light Protocol, see https://www.first.org/tlp/.
Please treat this document in accordance with the TLP assigned.

Description

Published: 2024-08-13T19:15:00
Vendor: Ivanti
Product: Virtual Traffic Manager (vTM)
CVE ID: CVE-2024-7593
CVSS3.0 Score[1]**:** 9.8 Critical
EPSS[2]**:** 0.094940000
For up to date EPSS score, click here: https://api.first.org/data/v1/epss?cve=CVE-2024-7593
Summary: Incorrect implementation of an authentication algorithm in Ivanti vTM other than versions 22.2R1 or 22.7R2 allows a remote unauthenticated attacker to bypass authentication of the admin panel.

Products Affected

- Ivanti vTM 22.2 - Patch available
- Ivanti vTM 22.3 - Patch expected week of August 19th
- Ivanti vTM 22.3R2 - Patch expected week of August 19th
- Ivanti vTM 22.5R1 - Patch expected week of August 19th
- Ivanti vTM 22.6R1 - Patch expected week of August 19th
- Ivanti vTM 22.7R1 - Patch available

Impact

Common Weakness Enumeration (CWE)[3]**:**
CWE-287 Improper Authentication
CWE-303 Incorrect Implementation of Authentication Algorithm

Present in CISA Known Exploited Vulnerability(KEV)[4] **catalog:** NO
Used by Ransomware Operators: Not Known

Recommendations

The NCSC strongly advises affected organisations to review the latest release notes and install the relevant updates from Ivanti. As temporary mitigation, Ivanti is recommending customers to limit admin access to the management interface or restrict access to trusted IP addresses

Additional recommendations and mitigation's for CVE-2024-7593 can be found in the link below:
https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Virtual-Traffic-Manager-vTM-CVE-2024-7593

[1] https://www.first.org/cvss/v3.0/specification-document
[2] https://www.first.org/epss/articles/prob_percentile_bins
[3] https://cwe.mitre.org/
[4] https://www.cisa.gov/known-exploited-vulnerabilities-catalog

DISCLAIMER: This document is provided “as is” without warranty of any kind, expressed or implied, including, but not limited to, the implied warranty of fitness for a particular purpose. NCSC-IE does not endorse any commercial product or service, referenced in this document or otherwise.

National Cyber Security Centre
Tom Johnson House,
Beggars Bush,
Dublin, D04 A068,
Ireland
Tel: +353 (0)1 6782333
Mail: certreport@ncsc.gov.ie
Web: ncsc.gov.ie
Twitter: ncsc_gov_ie
LinkedIn: ncsc-ie

An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre