Security Advisory 2024-078

Ivanti vTM Critical Authentication Bypass Vulnerability

August 14, 2024 — v1.0

TLP:CLEAR

History:

- *14/08/2024 — v1.0 – Initial publication*

Summary

On August 13, 2024, Ivanti disclosed a critical authentication bypass vulnerability, **CVE-2024-7593**, affecting the Ivanti Virtual Traffic Manager (vTM). This flaw allows remote, unauthenticated attackers to bypass authentication and create rogue administrator accounts, posing a significant security risk. The vulnerability is due to an incorrect implementation of the authentication algorithm.

Technical Details

The vulnerability, tracked as `CVE-2024-7593`, is caused by an incorrect authentication algorithm, enabling attackers to bypass the authentication process on Internet-exposed vTM admin panels. Exploitation could lead to unauthorised access and control over the affected system.

Affected Products

Product Name	Affected Version(s)	Resolved Version(s)	Patch Availability
Ivanti Virtual Traffic Manager	22.2	22.2R1	Available
Ivanti Virtual Traffic Manager	22.3	22.3R3	Week of August 19th
Ivanti Virtual Traffic Manager	22.3R2	22.3R3	Week of August 19th
Ivanti Virtual Traffic Manager	22.5R1	22.5R2	Week of August 19th
Ivanti Virtual Traffic Manager	22.6R1	22.6R2	Week of August 19th
Ivanti Virtual Traffic Manager	22.7R1	22.7R2	Available

Recommendations

CERT-EU strongly recommends updating to the latest patched version of Ivanti vTM. Additionally, restrict access to the management interface by binding it to an internal network or private IP address to reduce the attack surface.

References

[1] https://www.bleepingcomputer.com/news/security/ivanti-warns-of-critical-vtm-auth-bypass-with-public-exploit/