Corvit System Multan

Report Title :

CVE-2024-7593(Critical Flaw in Ivanti Virtual Traffic Manager Could Allow Rogue Admin Access)

Course : CEH (Certified ethical Hacker)

Submitted By : Fahad Usman

Submitted to : M.Bilal

Date : 18/08/2024

Table of contents

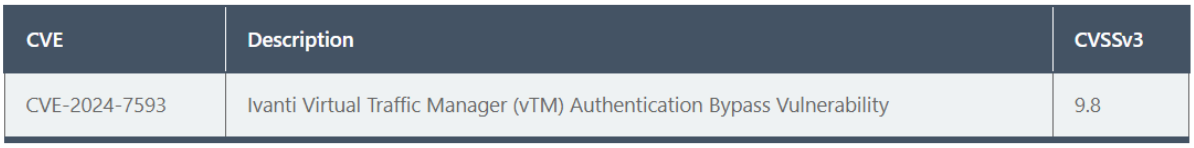
Topics

****

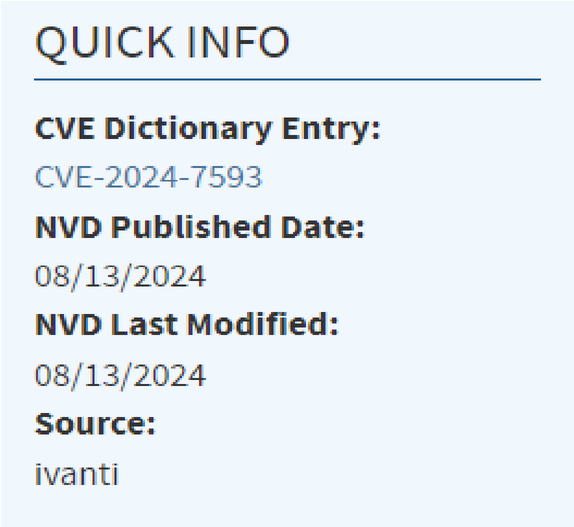
Background :

Ivanti released a patch for a critical severity authentication bypass vulnerability and a warning that exploit code is publicly available

On August 13, Ivanti released a security advisory to address a critical severity authentication bypass vulnerability in its Virtual Traffic Manager (vTM) product, a software-based application delivery controller (ADC).

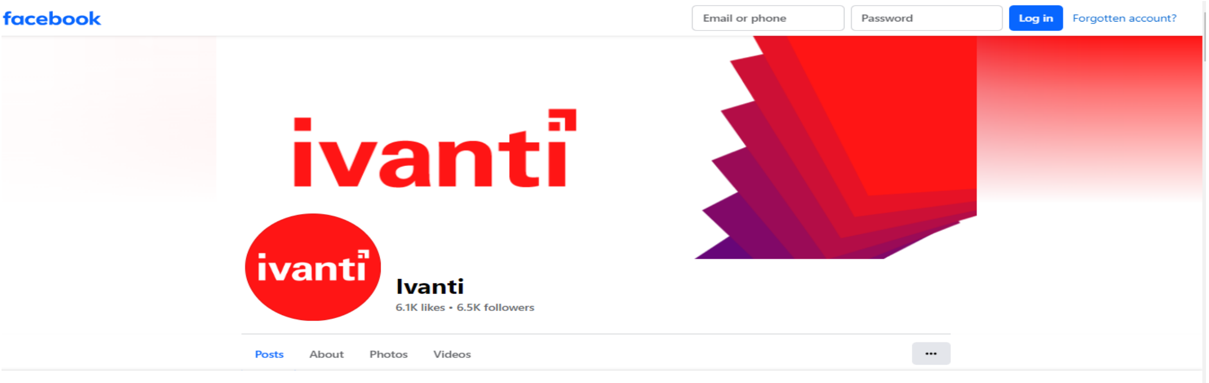


CVE	Description	CVSSv3
CVE-2024-7593	Ivanti Virtual Traffic Manager (vTM) Authentication Bypass Vulnerability	9.8



QUICK INFO

CVE Dictionary Entry:
CVE-2024-7593
NVD Published Date:
08/13/2024
NVD Last Modified:
08/13/2024
Source:
ivanti



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.

Analysis:

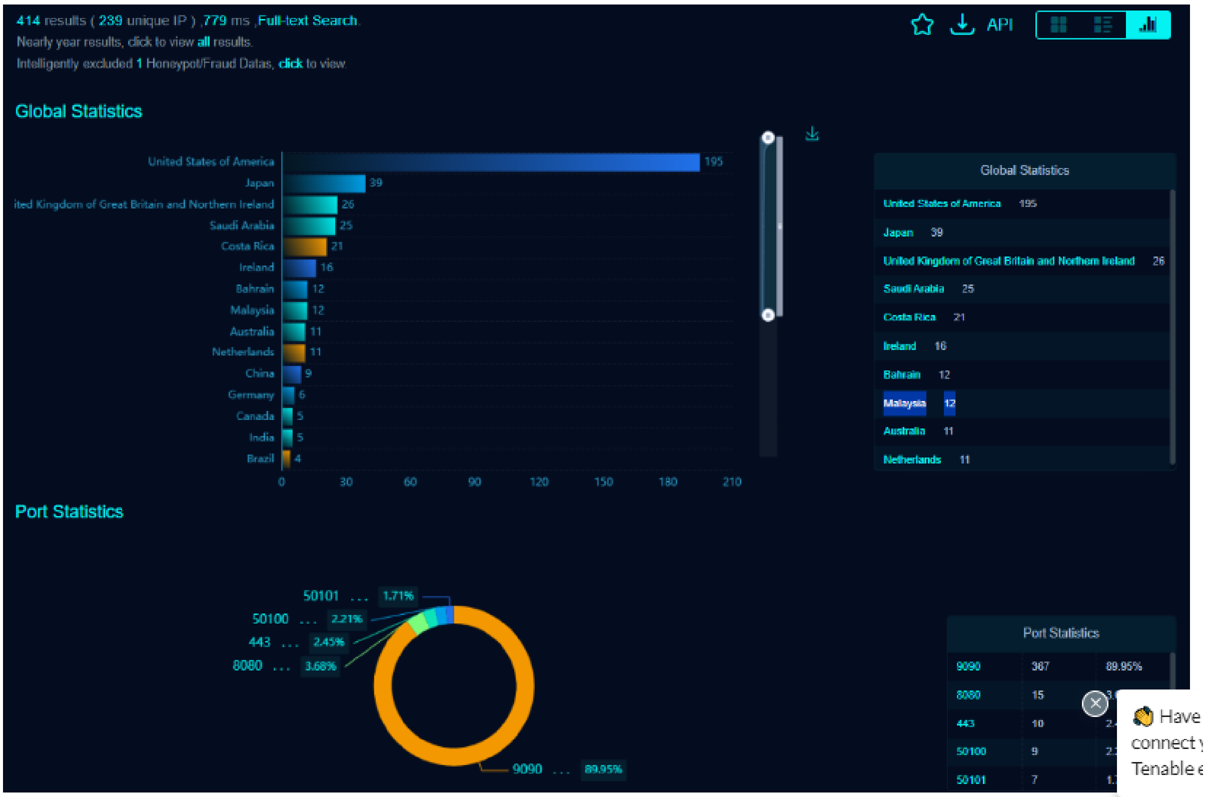
CVE-2024-7593 is a critical severity authentication bypass vulnerability. Exploitation of this flaw could allow an unauthenticated, remote attacker to create an administrator user. According to the advisory, access to the management interface of vTM is required in order to exploit this vulnerability.While Ivanti notes that no known exploitation has been observed for CVE-2024-7593, their advisory makes special note of publicly available exploit code.

Historical exploitation of Ivanti vulnerabilities

Ivanti has had a history of threat actors targeting their products, with one of the most prolific being attacks against their Ivanti Connect Secure (ICS) product, previously known as Pulse Connect Secure and Ivanti Policy Secure. In January, two zero-day vulnerabilities were exploited against ICS in a chained attack. Coincidentally enough, one of these vulnerabilities was an authentication bypass flaw. Within a few weeks of this release, Ivanti found several additional vulnerabilities impacting ICS, including another zero-day vulnerability (CVE-2024-21893) that had also been exploited in the wild. CVE-2023-46805 and CVE-2024-21887 were reportedly exploited by a threat actor tracked as UTA0178 and is believed to be a “Chinese nation-state level threat actor.” With threat actors, including nation-state aligned actors actively targeting Ivanti devices, it’s imperative that patching is prioritized.

Hundreds of Internet Facing Instances May Be Affected

Adding to the concern over the potential to exploit this vulnerability, a FOFA search lists more than 400 results tied to over 200 unique IPs that might be affected if patches or mitigations are not applied.



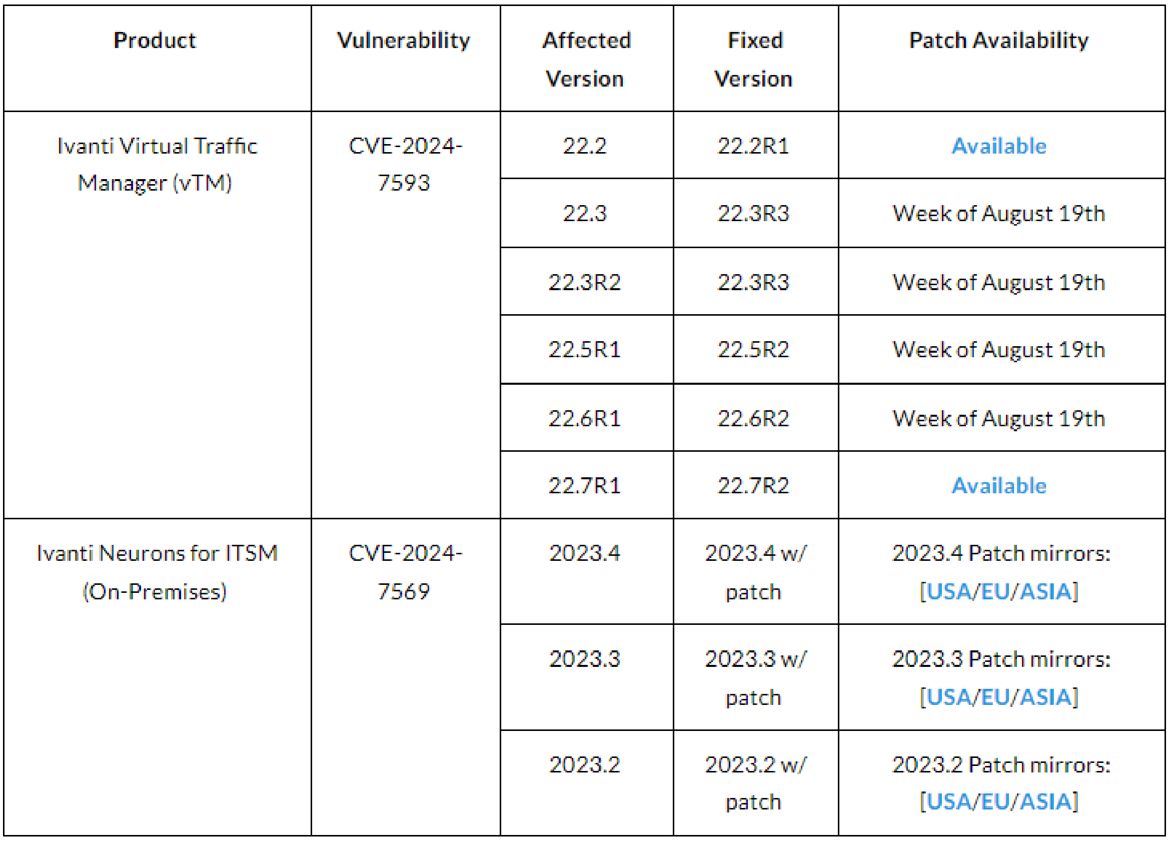
414 results (239 unique IP) ,779 ms ,Full-text Search.
Nearly year results, click to view all results.
Intelligently excluded 1 Honeypot/Fraud Datas, click to view.

Global Statistics	
United States of America	195
Japan	39
United Kingdom of Great Britain and Northern Ireland	26
Saudi Arabia	25
Costa Rica	21
Ireland	16
Bahrain	12
Malaysia	12
Australia	11
Netherlands	11

Port Statistics		
9090	367	89.95%
8080	15	3.
443	10	2.4
50100	9	2.2
50101	7	1.7

Affections :

Ivanti has stated that CVE-2024-7593 and CVE-2024-7569 have not been exploited so far, but they acknowledge that a proof of concept (PoC) is publicly available for CVE-2024-7593. Threat actors may target CVE-2024-7593 in the near term due to the publicly accessible PoC and ease of exploitation for vTM instances that are exposed to a threat actor.



Product	Vulnerability	Affected Version	Fixed Version	Patch Availability
Ivanti Virtual Traffic Manager (vTM)	CVE-2024-7593	22.2	22.2R1	Available
		22.3	22.3R3	Week of August 19th
		22.3R2	22.3R3	Week of August 19th
		22.5R1	22.5R2	Week of August 19th
		22.6R1	22.6R2	Week of August 19th
		22.7R1	22.7R2	Available
Ivanti Neurons for ITSM (On-Premises)	CVE-2024-7569	2023.4	2023.4 w/ patch	2023.4 Patch mirrors: [USA/EU/ASIA]
		2023.3	2023.3 w/ patch	2023.3 Patch mirrors: [USA/EU/ASIA]
		2023.2	2023.2 w/ patch	2023.2 Patch mirrors: [USA/EU/ASIA]

- Note: The patch has been applied to all Ivanti Neurons for ITSM Cloud instances as of August 4th. No further action is required for cloud customers.
  Please follow your organization's patching and testing guidelines to avoid any operational impact.

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.

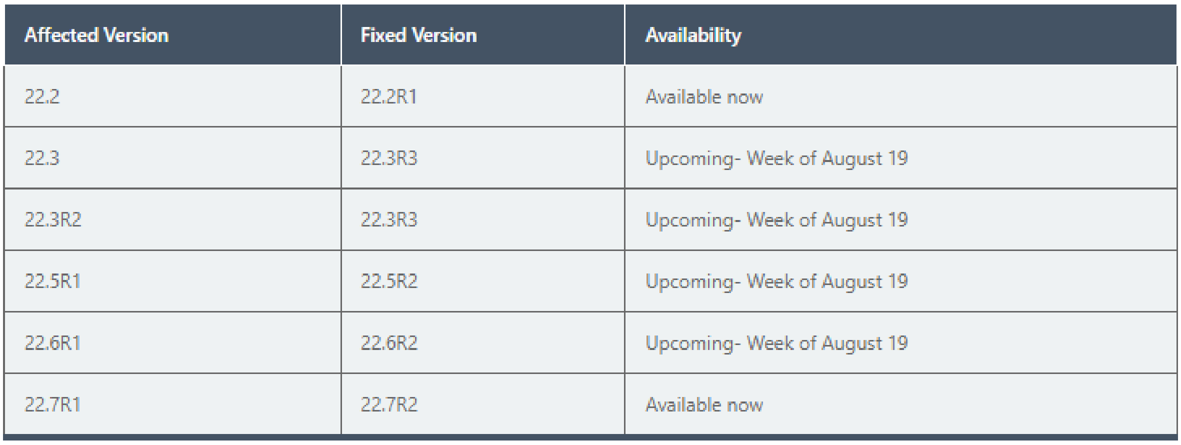
Proof Of Concept :

According to Ivanti's security advisory, a public proof-of-concept (PoC) is available for this vulnerability. While Tenable Research has not tested and confirmed a working exploit, we are aware of exploit code found on a popular site for public exploit scripts.

As attackers are keen to abuse targets with readily available exploit code, immediate patching or application of mitigation steps is recommended.

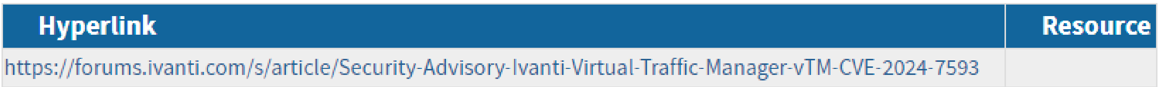
Solution and Hyperlink :

Ivanti has released some patches to address this vulnerability, with additional patch versions expected to be released the week of August 19. A summary of the patched versions can be found in the table below:

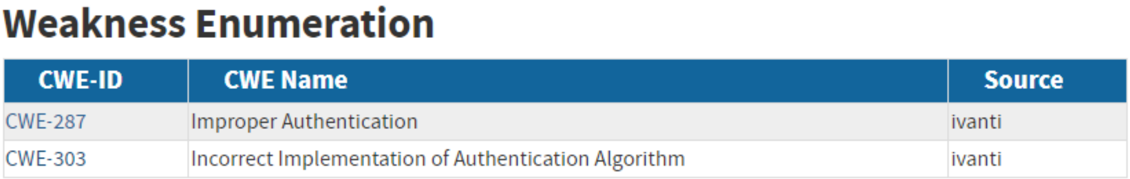


Affected Version	Fixed Version	Availability
22.2	22.2R1	Available now
22.3	22.3R3	Upcoming- Week of August 19
22.3R2	22.3R3	Upcoming- Week of August 19
22.5R1	22.5R2	Upcoming- Week of August 19
22.6R1	22.6R2	Upcoming- Week of August 19
22.7R1	22.7R2	Available now

For organizations that are not able to immediately patch this vulnerability, Ivanti does offer mitigation guidance. As access to the management interface is a requirement for exploitation, limiting access to this interface is recommended. Ivanti recommends to ensure that the management interface is bound to an internal network or private IP address. We recommend referring to Ivanti's security advisory for the most up to date information on patch availability and mitigation guidance.



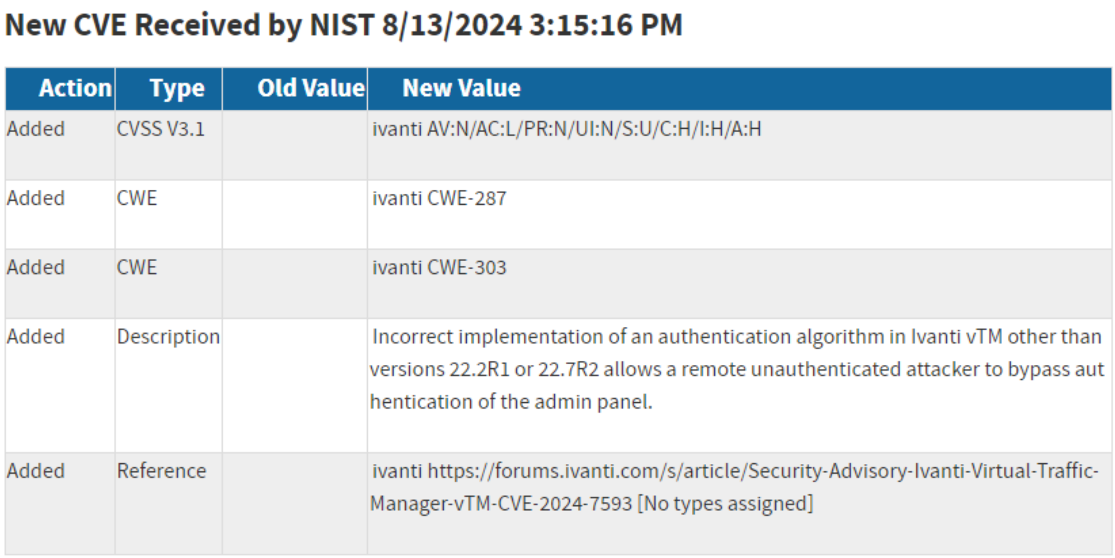
Hyperlink	Resource
https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Virtual-Traffic-Manager-vTM-CVE-2024-7593	



Weakness Enumeration

CWE-ID	CWE Name	Source
CWE-287	Improper Authentication	ivanti
CWE-303	Incorrect Implementation of Authentication Algorithm	ivanti

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.



New CVE Received by NIST 8/13/2024 3:15:16 PM

Action	Type	Old Value	New Value
Added	CVSS V3.1		ivanti AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Added	CWE		ivanti CWE-287
Added	CWE		ivanti CWE-303
Added	Description		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.
Added	Reference		ivanti https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Virtual-Traffic-Manager-vTM-CVE-2024-7593 [No types assigned]

Conclusion :

The CVE-2024-7593 is the vulnerabilities of the unauthorized attak and the work on it is started and Ivanti has stated that CVE-2024-7593 and CVE-2024-7569 have not been exploited so far, but they acknowledge that a proof of concept (PoC) is publicly available for CVE-2024-7593. Threat actors may target CVE-2024-7593 in the near term due to the publicly accessible PoC and ease of exploitation for vTM instances that are exposed to a threat actor.