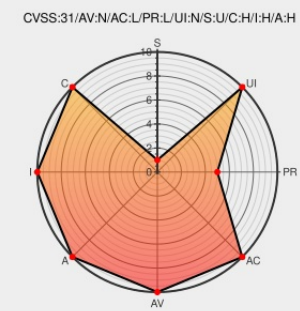
CVE-2021-35508

Published on: 09/01/2021 12:00:00 AM UTC

Last Modified on: 07/12/2022 05:42:00 PM UTC

CVE-2021-35508

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Aquariusnet from Terarecon contain the following vulnerability:

NMSAccess32.exe in TeraRecon AQNetClient 4.4.13 allows attackers to execute a malicious binary with SYSTEM privileges via a low-privileged user account. To exploit this, a low-privileged user must change the service configuration or overwrite the binary service.

CVE-2021-35508 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 8.8 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 8.5 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
ShareFile	terarecon.sharefile.com text/html	MISC terarecon.sharefile.com/d-s05c8b7792f354a2d8115789a02449c4a
CVE-2021-35508: Privilege Escalation via Weak Windows Service Permissions	www.linkedin.com text/html	MISC www.linkedin.com/pulse/cve-2021-35508-privilege-escalation-via-weak-windows-marshall-mba

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites 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 websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Terarecon	Aquariusnet	4.4.13	All	All	All

cpe:2.3:a:terarecon:aquariusnet:4.4.13:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-35508 : NMSAccess32.exe in TeraRecon AQNetClient 4.4.13 allows attackers to execute a malicious binary wit… twitter.com/i/web/status/1…	2021-09-01 14:05:47
@LinInfoSec	Pulse - CVE-2021-35508: terarecon.sharefile.com/d-s05c8b7792f3…	2021-09-01 16:50:57
@threatmeter	CVE-2021-35508 NMSAccess32.exe in TeraRecon AQNetClient 4.4.13 allows attackers to execute a malicious binary with… twitter.com/i/web/status/1…	2021-09-02 07:09:52

← Previous ID

Next ID→