|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | Mountable NFS Share | | |
| **Findings Categorization** | | | | |
| **Business Impact** | | High | **CVSS v4.0 Score** | 9.0 (High) |
| **CVSS Vector** | | CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:L/SI:L/SA:L | | |

Technical Description

An NFS (Network File System) share was found to be mountable without proper access restrictions from unauthorized clients. During network enumeration, the NFS service was discovered to have accessible exports without strong authentication measures, allowing arbitrary clients on the network to mount to the shared filesystems and extract information.

Business Impact Description

This configuration introduces several risks, including unauthorized data access, data exfiltration, or unwanted tampering by adversaries. In some configurations, remote users may even write to the share, leading to a full compromise of the data and systems relying on it.

This particular NFS share <INSERT CONTENTS>. Engineers further leveraged the exposed sensitive files to extract credentials and achieve an initial compromise into the affected host.

Affected Systems

* + Host:PORT/PROTOCOL (include hostname where possible)

Steps to Reproduce

During network enumeration, port scanning revealed the NFS share on host <HOSTNAME> and the showmount -e command revealed <DIRECTORY> that was accessible to everyone on the network without any authentication, allowing arbitrary clients on the network to mount to the shared filesystem and extract information.

Steps engineers took are shown below.

/Screenshot 1

Caption1

Engineers then attempted to mount the drive to view the contents.

/Screenshot 2

Caption 2

Mitigations

Ensure all network shares within the domain are restricted according to the business use cases with proper ACLs implemented. If there is a valid business case for exposing a network share to the general network, ensure that no confidential information of any kind is stored and implement continuous monitoring.

References

* **MITRE ATT&CK – Exfiltration Over NFS**
  + <https://attack.mitre.org/techniques/T1048/003/>
* **NIST SP 800-44 Rev. 1 – Guidelines on Securing Public Web Servers (includes file share considerations)**
  + <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-44r1.pdf>

{% endfor %}