|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | Misconfigured Sudoers File | | |
| **Findings Categorization** | | | | |
| **Business Impact** | | Medium | **CVSS v4.0 Score** | 7.6 (High) |
| **CVSS Vector** | | CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:L/SC:N/SI:N/SA:N | | |

Technical Description

Improperly configured sudo permissions can enable local users to escalate privileges to root, especially when arbitrary or exploitable binaries are made executable without a password. When an attacker can run such programs with elevated privileges, they may gain full control over the system.

In this particular engagement, engineers discovered that the local user account svcMosh on host <INSERT> was discovered to have NOPASSWD rights to execute the program /usr/bin/mosh-server as root without requiring authentication. This permission was confirmed by running sudo -l, which showed:

Business Impact Description

The use of default credentials on an administrative portal exposes the organization to threats and unauthorized system control. In this scenario, successful access allowed visibility into authentication data and internal system logs, which could be leveraged to further attack internal systems or impersonate users. The level of access that can be easily gained undermines the confidentiality and integrity of authentication infrastructure.

Affected Systems

* hostname:PORT/PROTOCOL (include affected endpoint or API where possible)
* Endpoint: [https://example.com/<ENDPOINT](https://example.com/%3cENDPOINT)>

Steps to Reproduce

After gaining a foothold on host <HOST>, engineers discovered the local user account svcMosh had NOPASSWD rights to execute the program /usr/bin/mosh-server as root without requiring authentication. This permission was confirmed by running sudo -l, which showed:

/Screenshot 1

Caption 1: Successful login using default credentials into the daloRADIUS operator interface.

Mitigations

* Immediately remove or change all default administrative credentials to strong passwords according to the recent NIST guidelines (detailed within the References section).
* Enforce strong password policies and mandatory password change at first login.
* Consider the business need to restrict access to administrative interfaces via firewall rules, IP allowlists, or VPN.
* Enable multi-factor authentication (MFA) for all privileged accounts.
* Periodically audit public-facing or internally exposed services for misconfigurations and default accounts.

References

* **OWASP – Authentication Cheat Sheet**
  + [**https://cheatsheetseries.owasp.org/cheatsheets/Authentication\_Cheat\_Sheet.html**](https://cheatsheetseries.owasp.org/cheatsheets/Authentication_Cheat_Sheet.html)
* **MITRE ATT&CK – T1078: Valid Accounts**
  + [**https://attack.mitre.org/techniques/T1078/**](https://attack.mitre.org/techniques/T1078/)
* **NIST SP 800-118 – Guide to Enterprise Password Management**
  + [**https://csrc.nist.gov/publications/detail/sp/800-118/final**](https://csrc.nist.gov/publications/detail/sp/800-118/final)