|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | Web Application with Default Credentials | | |
| **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

The presence of default credentials for exposed login interfaces presents a significant security risk. Default usernames and passwords are often widely documented and targeted by automated tools and attackers to gain unauthorized access. Applications that expose administrative or operator interfaces without enforcing proper credential hygiene are particularly vulnerable to compromise.

In this case, the web login interface for ***daloRADIUS, a RADIUS management platform***, was found to be exposed over the intranet. Upon reviewing the publicly available documentation, engineers identified the application's default credentials and successfully logged into the operator dashboard, which provided administrative functionality including user management, system logging and session tracking.

Engineers also noted that no password reset, or multi-factor authentication (MFA) was enforced upon login.

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

During a scan of the network, engineers identified and navigated to the exposed web interface: **https://<redacted-domain>/daloRADIUS**. After obtaining default credentials from research, engineers then logged in using the default credentials, gaining access to the administrative dashboard.

A screenshot of a computer

AI-generated content may be incorrect.

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

After obtaining access, engineers then enumerated the portal for any sensitive information that could lead to potential foothold opportunities as the default credentials enabled for full operator access to the application. Through this, engineers then recovered a password hash belonging to a local user svcMosh, which was then exported and cracked to reveal a cleartext password. The details of this process are explained in the **[Weak Password Recovered via Offline Hash Cracking]** finding.

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)