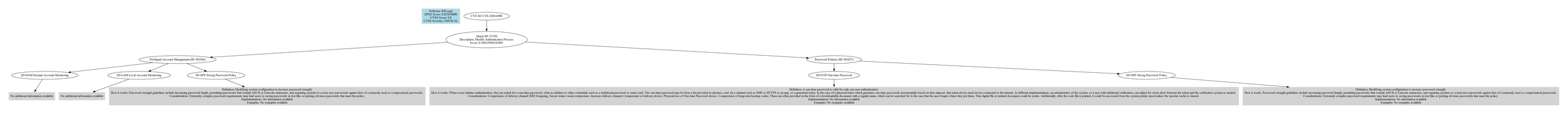
Software: RALogin
EPSS Score: 0.02670000
CVSS Score: 9.8
CVSS Severity: CRITICAL
CVE ID: CVE-2020-6990
Attack ID: T1556
Description: Modify Authentication Process
Score: 0.0862109036363401
Privileged Account Management (ID: M1026)
Password Policies (ID: M1027)
I3-DAM Domain Account Monitoring
I3-LAM Local Account Monitoring
I3-SPP Strong Password Policy
I3-OTP One-time Password
I3-SPP Strong Password Policy
No additional information available
No additional information available
Definition: Modifying system configuration to increase password strength.
How it works: Password strength guidelines include increasing password length, permitting passwords that contain ASCII or Unicode characters, and requiring systems to screen new passwords against lists of commonly used or compromised passwords.
Considerations: Extremely complex password requirements may lead users to saving passwords in text files or picking obvious passwords that meet the policy.
Implementations: No information available
Examples: No examples available
Definition: A one-time password is valid for only one user authentication.
How it works: When a user initiates authentication, they are asked for a one-time password, often in addition to other credentials such as a traditional password or smart card. The one-time password may be from a list provided in advance, sent via a channel such as SMS or HTTPS to an app, or a generated token. In the case of a physical token which generates one-time passwords incrementally based on time elapsed, that token device need not be connected to the internet. In different implementations, an administrator of the system, or a user with additional verification, can adjust for clock skew between the token and the verification system as needed.
Considerations: Compromise of delivery channel: SIM Swapping, Secure token virual compromise, Insecure delivery channel, Compromise of delivery device. Physical loss of One-time Password device. Compromise of long-term backup codes: These are often provided in the form of a downloadable document with a regular name, which can be searched for in the case that the user forgets where they put them. This digital file or printed document could be stolen. Additionally, after the code file is printed, it could be recovered from the system printer spool unless the spooler cache is cleared.
Implementations: No information available
Examples: No examples available
Definition: Modifying system configuration to increase password strength.
How it works: Password strength guidelines include increasing password length, permitting passwords that contain ASCII or Unicode characters, and requiring systems to screen new passwords against lists of commonly used or compromised passwords.
Considerations: Extremely complex password requirements may lead users to saving passwords in text files or picking obvious passwords that meet the policy.
Implementations: No information available
Examples: No examples available