**CWE and Risk Analysis:**

Below CWE’s related to logs are analyzed as part of the login misuse case.

[CWE-798](http://cwe.mitre.org/data/definitions/798) **- Use of Hard-coded Credentials**

**Parent of:**

[CWE-259](http://cwe.mitre.org/data/definitions/259) **- Use of Hard-coded Password** (specific for Password)

Hard-coded credential can be a valuable resource for an attacker that allows it to bypass the authentication that was configured. This creates a security hole which might be difficult for the system to detect, and even if detected might be difficult to fix. There exist to main variation, inbound (software contains an authentication mechanism that checks the input credential against a hard-coded set of credentials) and outbound (software connects to another system, and this system contains hard-coded credential for connecting components). This type of weakness is related to [CWE-344](https://cwe.mitre.org/data/definitions/344.html) Use of invariant value in Dynamically Changing Context, [CWE-671](https://cwe.mitre.org/data/definitions/671.html) Lack of administrator control over Security and [CWE-287](https://cwe.mitre.org/data/definitions/287.html) Improper Authentication. Related attach patterns [CAPEC-70](http://capec.mitre.org/data/definitions/70.html) Try common or Default Usernames and Passwords.

CWE-[307](https://cwe.mitre.org/data/definitions/307.html) **- Improper Restriction of Excessive Authentication Attempts**

Improper restriction of excessive authentication attempts can lead to brute force and dictionary attacks since it does not prevent multiple failed authentication attempts. This type of weakness is related to [CWE-799](https://cwe.mitre.org/data/definitions/799.html) Improper Control of Interaction Frequency and [CWE-287](https://cwe.mitre.org/data/definitions/287.html) Improper Authentication. We can see related vulnerabilities in [CVE-1999-1152](http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-1152). Related attack patterns can be seen in [CAPEC-16](http://capec.mitre.org/data/definitions/16.html) Dictionary-based Password Attack and [CAPEC-49](http://capec.mitre.org/data/definitions/49.html) Password Brute Forcing.