Severity

Medium

Analysis Summary

CVE-2021-39078 CVSS:4.1

IBM Security Guardium 10.5 stores user credentials in plain clear text which can be read by a local privileged user.

CVE-2021-39076 CVSS:3.7

IBM Security Guardium 10.5 and 11.3 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt sensitive information.

CVE-2021-39072 CVSS:5.1

IBM Security Guardium 11.3 could allow a remote attacker to obtain sensitive information, caused by the failure to properly enable HTTP Strict Transport Security. An attacker could exploit this vulnerability to obtain sensitive information using man in the middle techniques.

CVE-2021-39033 CVSS:4.3

IBM Sterling B2B Integrator Standard Edition 6.0.0.0 through 6.0.3.5 and 6.1.0.0 through 6.1.1.0 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system.

Impact

- Information Disclosure

Indicators Of Compromise

CVE

CVE-2021-39078 CVE-2021-39076 CVE-2021-39072 CVE-2021-39033

Affected Vendors

IBM

Affected Products

- IBM Security Guardium 10.5
- IBM Security Guardium 11.3
- IBM Sterling B2B Integrator 6.0.0.0
- IBM Sterling B2B Integrator 6.1.0.0
- IBM Sterling B2B Integrator 6.1.1.0
- IBM Sterling B2B Integrator 6.0.3.5

Remediation

Refer to IBM Security Advisory for patch, upgrade, or suggested workaround information.

CVE-2021-39078 CVE-2021-39076 CVE-2021-39072 CVE-2021-39033