Severity

High

Analysis Summary

CVE-2022-1256 CVSS:7.8

McAfee Agent for Windows could allow a local authenticated attacker to gain elevated privileges on the system, caused by improper privilege management in the repair functionality. By manipulating symbolic links, an attacker could exploit this vulnerability to carry out temporary file actions on the local user's %TEMP% directory with system privileges.

CVE-2022-1257 CVSS:6.1

McAfee Agent for Windows, McAfee Agent for macOS, and McAfee Agent for Linux could allow a local authenticated attacker to obtain sensitive information, caused by insecure storage of sensitive information in ma.db. An attacker could exploit this vulnerability to obtain sensitive information and use this information to launch further attacks against the affected system.

CVE-2022-1258 CVSS:8.4

McAfee ePolicy Orchestrator extension for McAfee Agent is vulnerable to SQL injection. A remote authenticated attacker could send specially-crafted SQL statements to the back-end database, which could allow the attacker to view, add, modify or delete information in the back-end database.

Impact

- Privilege Escalation
- Information Disclosure
- Data Manipulation

Indicator Of Compromise

CVE

- CVE-2022-1256
- CVE-2022-1257
- CVE-2022-1258

Affected Vendors

McAfee

Affected Products

- McAfee Agent 5.6.5 for Windows
- McAfee Agent 5.7.2 for Windows
- McAfee McAfee Agent (MA) for Linux 5.0.0
- McAfee McAfee Agent (MA) for Linux 5.0.6
- McAfee McAfee Agent (MA) for Linux 5.5.0
- McAfee McAfee Agent (MA) for Linux 5.5.1
- McAfee ePO Extension for McAfee Agent 4.0
- McAfee ePO extension for McAfee Agent 5.7.5

Remediation

Refer to McAfee Security Bulletin for patch, upgrade, or suggested workaround information.

McAfee Security