Severity

High

Analysis Summary

CVE-2022-23448 CVSS:7.3

Siemens SIMATIC Energy Manager Basic and SIMATIC Energy Manager PRO could allow a local authenticated attacker to execute arbitrary code on the system, caused by improperly assigning permissions to critical directories and files used by the application processes. By sending a specially-crafted request, an attacker could exploit this vulnerability to execute code with ADMINISTRATOR or even NT AUTHORITY/SYSTEM privileges.

CVE-2022-23449 CVSS:7.3

Siemens SIMATIC Energy Manager Basic and SIMATIC Energy Manager PRO could allow a local authenticated attacker to execute arbitrary code on the system, caused by improper loading of dynamic link libraries in the installer. By placing a malicious DLL file in one of the directories in the DLL search path, an attacker could exploit this vulnerability to execute code with elevated privileges.

CVE-2022-23450 CVSS:10

Siemens SIMATIC Energy Manager Basic and SIMATIC Energy Manager PRO could allow a remote attacker to execute arbitrary code on the system, caused by the unsafe deserialization of data. By sending a specially-crafted serialized object, an attacker could exploit this vulnerability to execute arbitrary code on the device with SYSTEM privileges.

Impact

- Code Execution

Indicators Of Compromise

CVE

- CVE-2022-23448
- CVE-2022-23449
- CVE-2022-23450

Affected Vendors

- Siemens

Affected Products

- Siemens SIMATIC Energy Manager Basic
- Siemens SIMATIC Energy Manager PRO

Remediation

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

Siemens Security Advisory