SSA-443402: Multiple SQL Injection Vulnerabilities in TeleControl Server Basic before V3.1.2.2

Publication Date: 2025-04-16
Last Update: 2025-04-16
Current Version: V1.0
CVSS v3.1 Base Score: 9.8
CVSS v4.0 Base Score: 9.3

SUMMARY

TeleControl Server Basic before V3.1.2.2 contains multiple SQL Injection vulnerabilities that could allow an attacker to read and write to the application's DB, cause denial of service and execute code in an OS shell with limited "NT AUTHORITY\NetworkService" permissions.

Siemens has conducted a root-cause analysis for potential SQL injection vulnerabilities and has identified the locations in the code base where the underlying legacy design pattern has been used in. TeleControl Server Basic V3.1.2.2 has fixed all occurrences in the affected product.

Siemens has released a new version for TeleControl Server Basic and recommends to update to the latest version.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
TeleControl Server Basic: All versions < V3.1.2.2 affected by all CVEs	Update to V3.1.2.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109987362/ See further recommendations from section Workarounds and Mitigations

WORKAROUNDS AND MITIGATIONS

Siemens has identified the following specific workarounds and mitigations that customers can apply to reduce the risk:

- Restrict access to port 8000 on the affected systems to trusted IP addresses only

Product-specific remediations or mitigations can be found in the section Affected Products and Solution. Please follow the General Security Recommendations.

GENERAL SECURITY RECOMMENDATIONS

As a general security measure, Siemens strongly recommends to protect network access to devices with appropriate mechanisms. In order to operate the devices in a protected IT environment, Siemens recommends to configure the environment according to Siemens' operational guidelines for Industrial Security (Download: https://www.siemens.com/cert/operational-guidelines-industrial-security), and to follow the recommendations in the product manuals. Additional information on Industrial Security by Siemens can be found at: https://www.siemens.com/industrialsecurity

PRODUCT DESCRIPTION

TeleControl Server Basic allows remote monitoring and control of plants via WAN/LAN.

VULNERABILITY DESCRIPTION

This chapter describes all vulnerabilities (CVE-IDs) addressed in this security advisory. Wherever applicable, it also documents the product-specific impact of the individual vulnerabilities.

Vulnerability CVE-2025-27495

The affected application is vulnerable to SQL injection through the internally used 'CreateTrace' method. This could allow an unauthenticated remote attacker to bypass authorization controls, to read from and write to the application's database and execute code with "NT AUTHORITY\NetworkService" permissions. A successful attack requires the attacker to be able to access port 8000 on a system where a vulnerable version of the affected application is executed on. (ZDI-CAN-25911)

CVSS v3.1 Base Score	9.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CVSS v4.0 Base Score	9.3
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:L/SI:L/SA:L
CWE	CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

Vulnerability CVE-2025-27539

The affected application is vulnerable to SQL injection through the internally used 'VerifyUser' method. This could allow an unauthenticated remote attacker to bypass authorization controls, to read from and write to the application's database and execute code with "NT AUTHORITY\NetworkService" permissions. A successful attack requires the attacker to be able to access port 8000 on a system where a vulnerable version of the affected application is executed on. (ZDI-CAN-25914)

CVSS v3.1 Base Score	9.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CVSS v4.0 Base Score	9.3
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:L/SI:L/SA:L
CWE	CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

Vulnerability CVE-2025-27540

The affected application is vulnerable to SQL injection through the internally used 'Authenticate' method. This could allow an unauthenticated remote attacker to bypass authorization controls, to read from and write to the application's database and execute code with "NT AUTHORITY\NetworkService" permissions. A successful attack requires the attacker to be able to access port 8000 on a system where a vulnerable version of the affected application is executed on. (ZDI-CAN-25913)

CVSS v3.1 Base Score	9.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CVSS v4.0 Base Score	9.3
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:L/SI:L/SA:L
CWE	CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

Vulnerability CVE-2025-29905

The affected application is vulnerable to SQL injection through the internally used 'RestoreFromBackup' method. This could allow an authenticated remote attacker to bypass authorization controls, to read from and write to the application's database and execute code with "NT AUTHORITY\NetworkService" permissions. A successful attack requires the attacker to be able to access port 8000 on a system where a vulnerable version of the affected application is executed on. (ZDI-CAN-25923)

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
CVSS v4.0 Base Score	8.7
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
CWE	CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

Vulnerability CVE-2025-30002

The affected application is vulnerable to SQL injection through the internally used 'UpdateConnectionVariables' method. This could allow an authenticated remote attacker to bypass authorization controls, to read from and write to the application's database and execute code with "NT AUTHORITY\NetworkService" permissions. A successful attack requires the attacker to be able to access port 8000 on a system where a vulnerable version of the affected application is executed on. (ZDI-CAN-25909)

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
CVSS v4.0 Base Score	8.7
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
CWE	CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

Vulnerability CVE-2025-30003

The affected application is vulnerable to SQL injection through the internally used 'UpdateProjectConnections' method. This could allow an authenticated remote attacker to bypass authorization controls, to read from and write to the application's database and execute code with "NT AUTHORITY\NetworkService" permissions. A successful attack requires the attacker to be able to access port 8000 on a system where a vulnerable version of the affected application is executed on. (ZDI-CAN-25910)

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
CVSS v4.0 Base Score	8.7
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
CWE	CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

Vulnerability CVE-2025-30030

The affected application is vulnerable to SQL injection through the internally used 'ImportDatabase' method. This could allow an authenticated remote attacker to bypass authorization controls, to read from and write to the application's database and execute code with "NT AUTHORITY\NetworkService" permissions. A successful attack requires the attacker to be able to access port 8000 on a system where a vulnerable version of the affected application is executed on. (ZDI-CAN-25924)

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
CVSS v4.0 Base Score	8.7
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
CWE	CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

Vulnerability CVE-2025-30031

The affected application is vulnerable to SQL injection through the internally used 'UpdateUsers' method. This could allow an authenticated remote attacker to bypass authorization controls, to read from and write to the application's database and execute code with "NT AUTHORITY\NetworkService" permissions. A successful attack requires the attacker to be able to access port 8000 on a system where a vulnerable version of the affected application is executed on. (ZDI-CAN-25922)

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
CVSS v4.0 Base Score	8.7
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
CWE	CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

Vulnerability CVE-2025-30032

The affected application is vulnerable to SQL injection through the internally used 'UpdateDatabaseSettings' method. This could allow an authenticated remote attacker to bypass authorization controls, to read from and write to the application's database and execute code with "NT AUTHORITY\NetworkService" permissions. A successful attack requires the attacker to be able to access port 8000 on a system where a vulnerable version of the affected application is executed on. (ZDI-CAN-25921)

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
CVSS v4.0 Base Score	8.7
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
CWE	CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

Vulnerability CVE-2025-31343

The affected application is vulnerable to SQL injection through the internally used 'UpdateTcmSettings' method. This could allow an authenticated remote attacker to bypass authorization controls, to read from and write to the application's database and execute code with "NT AUTHORITY\NetworkService" permissions. A successful attack requires the attacker to be able to access port 8000 on a system where a vulnerable version of the affected application is executed on. (ZDI-CAN-25920)

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
CVSS v4.0 Base Score	8.7
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
CWE	CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

Vulnerability CVE-2025-31349

The affected application is vulnerable to SQL injection through the internally used 'UpdateSmtpSettings' method. This could allow an authenticated remote attacker to bypass authorization controls, to read from and write to the application's database and execute code with "NT AUTHORITY\NetworkService" permissions. A successful attack requires the attacker to be able to access port 8000 on a system where a vulnerable version of the affected application is executed on. (ZDI-CAN-25919)

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
CVSS v4.0 Base Score	8.7
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
CWE	CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

Vulnerability CVE-2025-31350

The affected application is vulnerable to SQL injection through the internally used 'UpdateBufferingSettings' method. This could allow an authenticated remote attacker to bypass authorization controls, to read from and write to the application's database and execute code with "NT AUTHORITY\NetworkService" permissions. A successful attack requires the attacker to be able to access port 8000 on a system where a vulnerable version of the affected application is executed on. (ZDI-CAN-25918)

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
CVSS v4.0 Base Score	8.7
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
CWE	CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

Vulnerability CVE-2025-31351

The affected application is vulnerable to SQL injection through the internally used 'CreateProject' method. This could allow an authenticated remote attacker to bypass authorization controls, to read from and write to the application's database and execute code with "NT AUTHORITY\NetworkService" permissions. A successful attack requires the attacker to be able to access port 8000 on a system where a vulnerable version of the affected application is executed on. (ZDI-CAN-25917)

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
CVSS v4.0 Base Score	8.7
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
CWE	CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

Vulnerability CVE-2025-31352

The affected application is vulnerable to SQL injection through the internally used 'UpdateGateways' method. This could allow an authenticated remote attacker to bypass authorization controls, to read from and write to the application's database and execute code with "NT AUTHORITY\NetworkService" permissions. A successful attack requires the attacker to be able to access port 8000 on a system where a vulnerable version of the affected application is executed on. (ZDI-CAN-25915)

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
CVSS v4.0 Base Score	8.7
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
CWE	CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

Vulnerability CVE-2025-31353

The affected application is vulnerable to SQL injection through the internally used 'UpdateOpcSettings' method. This could allow an authenticated remote attacker to bypass authorization controls, to read from and write to the application's database and execute code with "NT AUTHORITY\NetworkService" permissions. A successful attack requires the attacker to be able to access port 8000 on a system where a vulnerable version of the affected application is executed on. (ZDI-CAN-25916)

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
CVSS v4.0 Base Score	8.7
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
CWE	CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

Vulnerability CVE-2025-32475

The affected application is vulnerable to SQL injection through the internally used 'UpdateProject' method. This could allow an authenticated remote attacker to bypass authorization controls, to read from and write to the application's database and execute code with "NT AUTHORITY\NetworkService" permissions. A successful attack requires the attacker to be able to access port 8000 on a system where a vulnerable version of the affected application is executed on. (ZDI-CAN-25912)

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
CVSS v4.0 Base Score	8.7
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
CWE	CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

Vulnerability CVE-2025-32822

The affected application is vulnerable to SQL injection through the internally used 'DeleteProject' method. This could allow an authenticated remote attacker to bypass authorization controls, to read from and write to the application's database and execute code with "NT AUTHORITY\NetworkService" permissions. A successful attack requires the attacker to be able to access port 8000 on a system where a vulnerable version of the affected application is executed on.

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
CVSS v4.0 Base Score	8.7
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
CWE	CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

Vulnerability CVE-2025-32823

The affected application is vulnerable to SQL injection through the internally used 'LockProject' method. This could allow an authenticated remote attacker to bypass authorization controls, to read from and write to the application's database and execute code with "NT AUTHORITY\NetworkService" permissions. A successful attack requires the attacker to be able to access port 8000 on a system where a vulnerable version of the affected application is executed on.

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
CVSS v4.0 Base Score	8.7
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
CWE	CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

Vulnerability CVE-2025-32824

The affected application is vulnerable to SQL injection through the internally used 'UnlockProject' method. This could allow an authenticated remote attacker to bypass authorization controls, to read from and write to the application's database and execute code with "NT AUTHORITY\NetworkService" permissions. A successful attack requires the attacker to be able to access port 8000 on a system where a vulnerable version of the affected application is executed on.

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
CVSS v4.0 Base Score	8.7
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
CWE	CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

Vulnerability CVE-2025-32825

The affected application is vulnerable to SQL injection through the internally used 'GetProjects' method. This could allow an authenticated remote attacker to bypass authorization controls, to read from and write to the application's database and execute code with "NT AUTHORITY\NetworkService" permissions. A successful attack requires the attacker to be able to access port 8000 on a system where a vulnerable version of the affected application is executed on.

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
CVSS v4.0 Base Score	8.7
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
CWE	CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

Vulnerability CVE-2025-32826

The affected application is vulnerable to SQL injection through the internally used 'GetActiveProjects' method. This could allow an authenticated remote attacker to bypass authorization controls, to read from and write to the application's database and execute code with "NT AUTHORITY\NetworkService" permissions. A successful attack requires the attacker to be able to access port 8000 on a system where a vulnerable version of the affected application is executed on.

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
CVSS v4.0 Base Score	8.7
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
CWE	CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

Vulnerability CVE-2025-32827

The affected application is vulnerable to SQL injection through the internally used 'ActivateProject' method. This could allow an authenticated remote attacker to bypass authorization controls, to read from and write to the application's database and execute code with "NT AUTHORITY\NetworkService" permissions. A successful attack requires the attacker to be able to access port 8000 on a system where a vulnerable version of the affected application is executed on.

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
CVSS v4.0 Base Score	8.7
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
CWE	CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

Vulnerability CVE-2025-32828

The affected application is vulnerable to SQL injection through the internally used 'UpdateProjectCrossCommunications' method. This could allow an authenticated remote attacker to bypass authorization controls, to read from and write to the application's database and execute code with "NT AUTHORITY\NetworkService" permissions. A successful attack requires the attacker to be able to access port 8000 on a system where a vulnerable version of the affected application is executed on.

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
CVSS v4.0 Base Score	8.7
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
CWE	CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

Vulnerability CVE-2025-32829

The affected application is vulnerable to SQL injection through the internally used 'LockProjectCrossCommunications' method. This could allow an authenticated remote attacker to bypass authorization controls, to read from and write to the application's database and execute code with "NT AUTHORITY\NetworkService" permissions. A successful attack requires the attacker to be able to access port 8000 on a system where a vulnerable version of the affected application is executed on.

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
CVSS v4.0 Base Score	8.7
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
CWE	CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

Vulnerability CVE-2025-32830

The affected application is vulnerable to SQL injection through the internally used 'UnlockProject' method. This could allow an authenticated remote attacker to bypass authorization controls, to read from and write to the application's database and execute code with "NT AUTHORITY\NetworkService" permissions. A successful attack requires the attacker to be able to access port 8000 on a system where a vulnerable version of the affected application is executed on.

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
CVSS v4.0 Base Score	8.7
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
CWE	CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

Vulnerability CVE-2025-32831

The affected application is vulnerable to SQL injection through the internally used 'UpdateProjectUserRights' method. This could allow an authenticated remote attacker to bypass authorization controls, to read from and write to the application's database and execute code with "NT AUTHORITY\NetworkService" permissions. A successful attack requires the attacker to be able to access port 8000 on a system where a vulnerable version of the affected application is executed on.

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
CVSS v4.0 Base Score	8.7
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
CWE	CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

Vulnerability CVE-2025-32832

The affected application is vulnerable to SQL injection through the internally used 'LockProjectUserRights' method. This could allow an authenticated remote attacker to bypass authorization controls, to read from and write to the application's database and execute code with "NT AUTHORITY\NetworkService" permissions. A successful attack requires the attacker to be able to access port 8000 on a system where a vulnerable version of the affected application is executed on.

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
CVSS v4.0 Base Score	8.7
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
CWE	CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

Vulnerability CVE-2025-32833

The affected application is vulnerable to SQL injection through the internally used 'UnlockProjectUserRights' method. This could allow an authenticated remote attacker to bypass authorization controls, to read from and write to the application's database and execute code with "NT AUTHORITY\NetworkService" permissions. A successful attack requires the attacker to be able to access port 8000 on a system where a vulnerable version of the affected application is executed on.

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
CVSS v4.0 Base Score	8.7
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
CWE	CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

Vulnerability CVE-2025-32834

The affected application is vulnerable to SQL injection through the internally used 'UpdateConnectionVariablesWithImport' method. This could allow an authenticated remote attacker to bypass authorization controls, to read from and write to the application's database and execute code with "NT AUTHORITY\NetworkService" permissions. A successful attack requires the attacker to be able to access port 8000 on a system where a vulnerable version of the affected application is executed on.

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
CVSS v4.0 Base Score	8.7
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
CWE	CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

Vulnerability CVE-2025-32835

The affected application is vulnerable to SQL injection through the internally used 'UpdateConnectionVariableArchivingBuffering' method. This could allow an authenticated remote attacker to bypass authorization controls, to read from and write to the application's database and execute code with "NT AUTHORITY\NetworkService" permissions. A successful attack requires the attacker to be able to access port 8000 on a system where a vulnerable version of the affected application is executed on.

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
CVSS v4.0 Base Score	8.7
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
CWE	CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

Vulnerability CVE-2025-32836

The affected application is vulnerable to SQL injection through the internally used 'GetConnectionVariables' method. This could allow an authenticated remote attacker to bypass authorization controls, to read from and write to the application's database and execute code with "NT AUTHORITY\NetworkService" permissions. A successful attack requires the attacker to be able to access port 8000 on a system where a vulnerable version of the affected application is executed on.

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
CVSS v4.0 Base Score	8.7
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
CWE	CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

Vulnerability CVE-2025-32837

The affected application is vulnerable to SQL injection through the internally used 'GetActiveConnectionVariables' method. This could allow an authenticated remote attacker to bypass authorization controls, to read from and write to the application's database and execute code with "NT AUTHORITY\NetworkService" permissions. A successful attack requires the attacker to be able to access port 8000 on a system where a vulnerable version of the affected application is executed on.

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
CVSS v4.0 Base Score	8.7
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
CWE	CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

Vulnerability CVE-2025-32838

The affected application is vulnerable to SQL injection through the internally used 'ImportConnectionVariables' method. This could allow an authenticated remote attacker to bypass authorization controls, to read from and write to the application's database and execute code with "NT AUTHORITY\NetworkService" permissions. A successful attack requires the attacker to be able to access port 8000 on a system where a vulnerable version of the affected application is executed on.

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
CVSS v4.0 Base Score	8.7
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
CWE	CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

Vulnerability CVE-2025-32839

The affected application is vulnerable to SQL injection through the internally used 'GetGateways' method. This could allow an authenticated remote attacker to bypass authorization controls, to read from and write to the application's database and execute code with "NT AUTHORITY\NetworkService" permissions. A successful attack requires the attacker to be able to access port 8000 on a system where a vulnerable version of the affected application is executed on.

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
CVSS v4.0 Base Score	8.7
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
CWE	CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

Vulnerability CVE-2025-32840

The affected application is vulnerable to SQL injection through the internally used 'LockGateway' method. This could allow an authenticated remote attacker to bypass authorization controls, to read from and write to the application's database and execute code with "NT AUTHORITY\NetworkService" permissions. A successful attack requires the attacker to be able to access port 8000 on a system where a vulnerable version of the affected application is executed on.

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
CVSS v4.0 Base Score	8.7
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
CWE	CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

Vulnerability CVE-2025-32841

The affected application is vulnerable to SQL injection through the internally used 'UnlockGateway' method. This could allow an authenticated remote attacker to bypass authorization controls, to read from and write to the application's database and execute code with "NT AUTHORITY\NetworkService" permissions. A successful attack requires the attacker to be able to access port 8000 on a system where a vulnerable version of the affected application is executed on.

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
CVSS v4.0 Base Score	8.7
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
CWE	CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

Vulnerability CVE-2025-32842

The affected application is vulnerable to SQL injection through the internally used 'GetUsers' method. This could allow an authenticated remote attacker to bypass authorization controls, to read from and write to the application's database and execute code with "NT AUTHORITY\NetworkService" permissions. A successful attack requires the attacker to be able to access port 8000 on a system where a vulnerable version of the affected application is executed on.

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
CVSS v4.0 Base Score	8.7
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
CWE	CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

Vulnerability CVE-2025-32843

The affected application is vulnerable to SQL injection through the internally used 'LockUser' method. This could allow an authenticated remote attacker to bypass authorization controls, to read from and write to the application's database and execute code with "NT AUTHORITY\NetworkService" permissions. A successful attack requires the attacker to be able to access port 8000 on a system where a vulnerable version of the affected application is executed on.

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
CVSS v4.0 Base Score	8.7
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
CWE	CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

Vulnerability CVE-2025-32844

The affected application is vulnerable to SQL injection through the internally used 'UnlockUser' method. This could allow an authenticated remote attacker to bypass authorization controls, to read from and write to the application's database and execute code with "NT AUTHORITY\NetworkService" permissions. A successful attack requires the attacker to be able to access port 8000 on a system where a vulnerable version of the affected application is executed on.

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
CVSS v4.0 Base Score	8.7
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
CWE	CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

Vulnerability CVE-2025-32845

The affected application is vulnerable to SQL injection through the internally used 'UpdateGeneralSettings' method. This could allow an authenticated remote attacker to bypass authorization controls, to read from and write to the application's database and execute code with "NT AUTHORITY\NetworkService" permissions. A successful attack requires the attacker to be able to access port 8000 on a system where a vulnerable version of the affected application is executed on.

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
CVSS v4.0 Base Score	8.7
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
CWE	CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

Vulnerability CVE-2025-32846

The affected application is vulnerable to SQL injection through the internally used 'LockGeneralSettings' method. This could allow an authenticated remote attacker to bypass authorization controls, to read from and write to the application's database and execute code with "NT AUTHORITY\NetworkService" permissions. A successful attack requires the attacker to be able to access port 8000 on a system where a vulnerable version of the affected application is executed on.

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
CVSS v4.0 Base Score	8.7
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
CWE	CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

Vulnerability CVE-2025-32847

The affected application is vulnerable to SQL injection through the internally used 'UnlockGeneralSettings' method. This could allow an authenticated remote attacker to bypass authorization controls, to read from and write to the application's database and execute code with "NT AUTHORITY\NetworkService" permissions. A successful attack requires the attacker to be able to access port 8000 on a system where a vulnerable version of the affected application is executed on.

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
CVSS v4.0 Base Score	8.7
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
CWE	CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

Vulnerability CVE-2025-32848

The affected application is vulnerable to SQL injection through the internally used 'LockSmtpSettings' method. This could allow an authenticated remote attacker to bypass authorization controls, to read from and write to the application's database and execute code with "NT AUTHORITY\NetworkService" permissions. A successful attack requires the attacker to be able to access port 8000 on a system where a vulnerable version of the affected application is executed on.

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
CVSS v4.0 Base Score	8.7
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
CWE	CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

Vulnerability CVE-2025-32849

The affected application is vulnerable to SQL injection through the internally used 'UnlockSmtpSettings' method. This could allow an authenticated remote attacker to bypass authorization controls, to read from and write to the application's database and execute code with "NT AUTHORITY\NetworkService" permissions. A successful attack requires the attacker to be able to access port 8000 on a system where a vulnerable version of the affected application is executed on.

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
CVSS v4.0 Base Score	8.7
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
CWE	CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

Vulnerability CVE-2025-32850

The affected application is vulnerable to SQL injection through the internally used 'LockTcmSettings' method. This could allow an authenticated remote attacker to bypass authorization controls, to read from and write to the application's database and execute code with "NT AUTHORITY\NetworkService" permissions. A successful attack requires the attacker to be able to access port 8000 on a system where a vulnerable version of the affected application is executed on.

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
CVSS v4.0 Base Score	8.7
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
CWE	CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

Vulnerability CVE-2025-32851

The affected application is vulnerable to SQL injection through the internally used 'UnlockTcmSettings' method. This could allow an authenticated remote attacker to bypass authorization controls, to read from and write to the application's database and execute code with "NT AUTHORITY\NetworkService" permissions. A successful attack requires the attacker to be able to access port 8000 on a system where a vulnerable version of the affected application is executed on.

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
CVSS v4.0 Base Score	8.7
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
CWE	CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

Vulnerability CVE-2025-32852

The affected application is vulnerable to SQL injection through the internally used 'LockDatabaseSettings' method. This could allow an authenticated remote attacker to bypass authorization controls, to read from and write to the application's database and execute code with "NT AUTHORITY\NetworkService" permissions. A successful attack requires the attacker to be able to access port 8000 on a system where a vulnerable version of the affected application is executed on.

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
CVSS v4.0 Base Score	8.7
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
CWE	CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

Vulnerability CVE-2025-32853

The affected application is vulnerable to SQL injection through the internally used 'UnlockDatabaseSettings' method. This could allow an authenticated remote attacker to bypass authorization controls, to read from and write to the application's database and execute code with "NT AUTHORITY\NetworkService" permissions. A successful attack requires the attacker to be able to access port 8000 on a system where a vulnerable version of the affected application is executed on.

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
CVSS v4.0 Base Score	8.7
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
CWE	CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

Vulnerability CVE-2025-32854

The affected application is vulnerable to SQL injection through the internally used 'LockOpcSettings' method. This could allow an authenticated remote attacker to bypass authorization controls, to read from and write to the application's database and execute code with "NT AUTHORITY\NetworkService" permissions. A successful attack requires the attacker to be able to access port 8000 on a system where a vulnerable version of the affected application is executed on.

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
CVSS v4.0 Base Score	8.7
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
CWE	CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

Vulnerability CVE-2025-32855

The affected application is vulnerable to SQL injection through the internally used 'UnlockOpcSettings' method. This could allow an authenticated remote attacker to bypass authorization controls, to read from and write to the application's database and execute code with "NT AUTHORITY\NetworkService" permissions. A successful attack requires the attacker to be able to access port 8000 on a system where a vulnerable version of the affected application is executed on.

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
CVSS v4.0 Base Score	8.7
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
CWE	CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

Vulnerability CVE-2025-32856

The affected application is vulnerable to SQL injection through the internally used 'LockBufferingSettings' method. This could allow an authenticated remote attacker to bypass authorization controls, to read from and write to the application's database and execute code with "NT AUTHORITY\NetworkService" permissions. A successful attack requires the attacker to be able to access port 8000 on a system where a vulnerable version of the affected application is executed on.

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
CVSS v4.0 Base Score	8.7
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
CWE	CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

Vulnerability CVE-2025-32857

The affected application is vulnerable to SQL injection through the internally used 'UnlockBufferingSettings' method. This could allow an authenticated remote attacker to bypass authorization controls, to read from and write to the application's database and execute code with "NT AUTHORITY\NetworkService" permissions. A successful attack requires the attacker to be able to access port 8000 on a system where a vulnerable version of the affected application is executed on.

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
CVSS v4.0 Base Score	8.7
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
CWE	CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

Vulnerability CVE-2025-32858

The affected application is vulnerable to SQL injection through the internally used 'UpdateWebServerGatewaySettings' method. This could allow an authenticated remote attacker to bypass authorization controls, to read from and write to the application's database and execute code with "NT AUTHORITY\NetworkService" permissions. A successful attack requires the attacker to be able to access port 8000 on a system where a vulnerable version of the affected application is executed on.

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
CVSS v4.0 Base Score	8.7
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
CWE	CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

Vulnerability CVE-2025-32859

The affected application is vulnerable to SQL injection through the internally used 'LockWebServerGatewaySettings' method. This could allow an authenticated remote attacker to bypass authorization controls, to read from and write to the application's database and execute code with "NT AUTHORITY\NetworkService" permissions. A successful attack requires the attacker to be able to access port 8000 on a system where a vulnerable version of the affected application is executed on.

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
CVSS v4.0 Base Score	8.7
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
CWE	CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

Vulnerability CVE-2025-32860

The affected application is vulnerable to SQL injection through the internally used 'UnlockWebServerGatewaySettings' method. This could allow an authenticated remote attacker to bypass authorization controls, to read from and write to the application's database and execute code with "NT AUTHORITY\NetworkService" permissions. A successful attack requires the attacker to be able to access port 8000 on a system where a vulnerable version of the affected application is executed on.

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
CVSS v4.0 Base Score	8.7
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
CWE	CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

Vulnerability CVE-2025-32861

The affected application is vulnerable to SQL injection through the internally used 'UpdateTraceLevelSettings' method. This could allow an authenticated remote attacker to bypass authorization controls, to read from and write to the application's database and execute code with "NT AUTHORITY\NetworkService" permissions. A successful attack requires the attacker to be able to access port 8000 on a system where a vulnerable version of the affected application is executed on.

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
CVSS v4.0 Base Score	8.7
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
CWE	CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

Vulnerability CVE-2025-32862

The affected application is vulnerable to SQL injection through the internally used 'LockTraceLevelSettings' method. This could allow an authenticated remote attacker to bypass authorization controls, to read from and write to the application's database and execute code with "NT AUTHORITY\NetworkService" permissions. A successful attack requires the attacker to be able to access port 8000 on a system where a vulnerable version of the affected application is executed on.

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
CVSS v4.0 Base Score	8.7
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
CWE	CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

Vulnerability CVE-2025-32863

The affected application is vulnerable to SQL injection through the internally used 'UnlockTraceLevelSettings' method. This could allow an authenticated remote attacker to bypass authorization controls, to read from and write to the application's database and execute code with "NT AUTHORITY\NetworkService" permissions. A successful attack requires the attacker to be able to access port 8000 on a system where a vulnerable version of the affected application is executed on.

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
CVSS v4.0 Base Score	8.7
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
CWE	CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

Vulnerability CVE-2025-32864

The affected application is vulnerable to SQL injection through the internally used ‘GetSettings’ method. This could allow an authenticated remote attacker to bypass authorization controls, to read from and write to the application’s database and execute code with “NT AUTHORITY\NetworkService” permissions. A successful attack requires the attacker to be able to access port 8000 on a system where a vulnerable version of the affected application is executed on.

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
CVSS v4.0 Base Score	8.7
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
CWE	CWE-89: Improper Neutralization of Special Elements used in an SQL Command (’SQL Injection’)

Vulnerability CVE-2025-32865

The affected application is vulnerable to SQL injection through the internally used ‘CreateLog’ method. This could allow an authenticated remote attacker to bypass authorization controls, to read from and write to the application’s database and execute code with “NT AUTHORITY\NetworkService” permissions. A successful attack requires the attacker to be able to access port 8000 on a system where a vulnerable version of the affected application is executed on.

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
CVSS v4.0 Base Score	8.7
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
CWE	CWE-89: Improper Neutralization of Special Elements used in an SQL Command (’SQL Injection’)

Vulnerability CVE-2025-32866

The affected application is vulnerable to SQL injection through the internally used ‘GetLogs’ method. This could allow an authenticated remote attacker to bypass authorization controls, to read from and write to the application’s database and execute code with “NT AUTHORITY\NetworkService” permissions. A successful attack requires the attacker to be able to access port 8000 on a system where a vulnerable version of the affected application is executed on.

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
CVSS v4.0 Base Score	8.7
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
CWE	CWE-89: Improper Neutralization of Special Elements used in an SQL Command (’SQL Injection’)

Vulnerability CVE-2025-32867

The affected application is vulnerable to SQL injection through the internally used ‘CreateBackup’ method. This could allow an authenticated remote attacker to bypass authorization controls, to read from and write to the application’s database and execute code with “NT AUTHORITY\NetworkService” permissions. A successful attack requires the attacker to be able to access port 8000 on a system where a vulnerable version of the affected application is executed on.

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
CVSS v4.0 Base Score	8.7
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
CWE	CWE-89: Improper Neutralization of Special Elements used in an SQL Command (’SQL Injection’)

Vulnerability CVE-2025-32868

The affected application is vulnerable to SQL injection through the internally used 'ExportCertificate' method. This could allow an authenticated remote attacker to bypass authorization controls, to read from and write to the application's database and execute code with "NT AUTHORITY\NetworkService" permissions. A successful attack requires the attacker to be able to access port 8000 on a system where a vulnerable version of the affected application is executed on.

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
CVSS v4.0 Base Score	8.7
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
CWE	CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

Vulnerability CVE-2025-32869

The affected application is vulnerable to SQL injection through the internally used 'ImportCertificate' method. This could allow an authenticated remote attacker to bypass authorization controls, to read from and write to the application's database and execute code with "NT AUTHORITY\NetworkService" permissions. A successful attack requires the attacker to be able to access port 8000 on a system where a vulnerable version of the affected application is executed on.

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
CVSS v4.0 Base Score	8.7
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
CWE	CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

Vulnerability CVE-2025-32870

The affected application is vulnerable to SQL injection through the internally used 'GetTraces' method. This could allow an authenticated remote attacker to bypass authorization controls, to read from and write to the application's database and execute code with "NT AUTHORITY\NetworkService" permissions. A successful attack requires the attacker to be able to access port 8000 on a system where a vulnerable version of the affected application is executed on.

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
CVSS v4.0 Base Score	8.7
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
CWE	CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

Vulnerability CVE-2025-32871

The affected application is vulnerable to SQL injection through the internally used 'MigrateDatabase' method. This could allow an authenticated remote attacker to bypass authorization controls, to read from and write to the application's database and execute code with "NT AUTHORITY\NetworkService" permissions. A successful attack requires the attacker to be able to access port 8000 on a system where a vulnerable version of the affected application is executed on.

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
CVSS v4.0 Base Score	8.7
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
CWE	CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

Vulnerability CVE-2025-32872

The affected application is vulnerable to SQL injection through the internally used 'GetOverview' method. This could allow an authenticated remote attacker to bypass authorization controls, to read from and write to the application's database and execute code with "NT AUTHORITY\NetworkService" permissions. A successful attack requires the attacker to be able to access port 8000 on a system where a vulnerable version of the affected application is executed on.

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
CVSS v4.0 Base Score	8.7
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
CWE	CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

ACKNOWLEDGMENTS

Siemens thanks the following party for its efforts:

- Trend Micro Zero Day Initiative for coordinated disclosure of CVE-2025-32475, CVE-2025-31353, CVE-2025-31352, CVE-2025-31351, CVE-2025-31350, CVE-2025-31349, CVE-2025-31343, CVE-2025-30032, CVE-2025-30031, CVE-2025-30030, CVE-2025-30003, CVE-2025-30002, CVE-2025-29905, CVE-2025-27540, CVE-2025-27539, CVE-2025-27495

ADDITIONAL INFORMATION

Siemens has conducted a root-cause analysis for potential SQL injection vulnerabilities and has identified the locations in the code base where the underlying legacy design pattern has been used in. TeleControl Server Basic V3.1.2.2 has fixed all occurrences in the affected product.

For further inquiries on security vulnerabilities in Siemens products and solutions, please contact the Siemens ProductCERT:

https://www.siemens.com/cert/advisories

HISTORY DATA

V1.0 (2025-04-16): Publication Date

TERMS OF USE