jTag Labs

VULNERABILITY DISCLOSURE

CATEREASE

OUR MISSION

At jTag Labs, our mission is to enhance safety by identifying and informing about vulnerabilities and security issues in technology. Driven by our dedication to transparency and accountability, we believe that knowledge and understanding should be universally accessible, empowering individuals, communities, and corporations alike to protect themselves in an increasingly digital world. Through our work, we aim to foster a culture of security awareness and promote a safer, more informed society.

Austin Henderson
CerebralStud

Cstar

Calvin Star
Skelet4r

OVERVIEW

Caterease is a comprehensive event management solution widely used by hospitality and event companies to streamline their operations. Designed for on-premises deployment, it caters to various businesses such as catering companies, restaurants, hotels, banquet halls, event centers, and entertainment venues.

The application provides a robust suite of tools to manage a wide range of event-related activities, including event booking, client and contact management, detailed catering and menu planning, staffing and scheduling, and payment tracking.

Given its extensive use, **Caterease** handles a significant amount of sensitive information, such as client personal details, event specifics, personal staff information, revenue and financial data, payment information, and much more. This critical information is essential for the day-to-day operations of businesses that rely on **Caterease**, making its security paramount.

The primary objective of this report is to bring attention to critical security vulnerabilities identified in **Caterease**, aligning with our mission to enhance safety and promote security awareness.

By detailing these vulnerabilities, we aim to raise awareness among **Horizon Business Services Inc.**, the software's vendor, as well as its clients and users. It is our hope that this information will prompt **Horizon Business Services** to take swift action in addressing these issues through official patches and updates. Additionally, we provide temporary mitigation strategies that users can implement to protect themselves against some of these vulnerabilities until permanent fixes are released.

At the time of releasing this Vulnerability Disclosure, **CVE-2024-38881** through **CVE-2024-38891** are all still actively exploitable within version **16.0.1.1663** through **24.0.1.2405** of **Caterease**, and there are no patches currently available to remediate these issues.

COMMON TERMS/ABBREVIATIONS

CAPEC - Common Attack Pattern Enumeration and Classification

CVE - Common Vulnerabilities and Exposures

CVSS - Common Vulnerability Scoring System

CWE - Common Weakness Enumeration

DBO - Database Owner

DoS - Denial of Service

MITM - Man-In-The-Middle

OS - Operating System

SQL - Structured Query Langage

TCP - Transmission Control Protocol

TDS - Tabular Data Stream

UID - User Identifier

CVE-2024-38881 - OVERVIEW

CWE-759

CVE-2024-38881: An issue in Horizon Business Services Inc. Caterease allows a remote attacker to perform a Rainbow Table Password cracking attack due to the use of one-way hashes without salts when storing user passwords.

Vulnerability Type: CWE-759: Use of a One-Way Hash without a Salt

Vendor of the Product: Horizon Business Services Inc.
Affected Product: Caterease
Affected Versions: 16.0.1.1663 through 24.0.1.2405

Attack Vector: Remote
Attack Type: CAPEC-55: Rainbow Table Password Cracking

Vulnerability Summary: Caterease stores user password hashes without salts, making them vulnerable to rainbow table attacks. This vulnerability arises because the application fails to use a cryptographic salt when hashing passwords, a critical security measure designed to protect against precomputed hash attacks. An attacker can exploit this vulnerability by precomputing hash values for a wide range of possible passwords and then comparing them to the stored hashes. Once a match is found, the original password can be recovered, leading to unauthorized access to user accounts.

The exposure of unsalted hashes not only compromises the security of the Caterease accounts but also facilitates further attacks, such as credential stuffing on other systems where users may have reused passwords. The lack of salting significantly compromises user account confidentiality and can result in privilege escalation, where an attacker gains access to higher-privilege accounts.

CVSS Base Score: Medium Risk - 6.5
CVSS v3.1 Vector: AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

Exploitability Metrics:
Attack Vector (AV): Adjacent Network
Attack Complexity (AC): Low
Privileges Required (PR): None
User Interaction (UI): None
Scope (S): Unchanged

Impact Metrics:
Confidentiality (C): High
Integrity (I): None
Availability (A): None

End of Overview

CVE-2024-38881 - IMPACT

CWE-759

Confidentiality: HIGH

The CWE-759 vulnerability, involving the use of one-way hashes without salts, poses a significant risk to confidentiality, warranting a high severity rating. Exploiting this vulnerability allows an attacker to recover user passwords stored within the **Caterease** database using rainbow table password cracking techniques. Once exploited, an attacker can gain unauthorized access to the **Caterease** application using the decrypted passwords, gaining the privileges of those users.

End of Impact Statements

CVE-2024-38881 - RISK SUMMARY

CWE-759

The use of one-way password hashes without salts can lead to the compromise of any **Caterease** user account, resulting in a complete breach of confidentiality within the application. Once an attacker compromises a user account, they can perform any and all actions as that user. These actions include, but are not limited to:

1. Password Cracking: Unsalted hashes make it easier for attackers to use precomputed hash tables (rainbow tables) to crack passwords. This can lead to unauthorized access to user accounts within the **Caterease** application.

2. Account Takeover: Once passwords are cracked, attackers can take over user accounts, potentially leading to misuse of those accounts for malicious purposes within the application.

3. Data Breach: Cracked passwords can be used to access sensitive information stored within the application, such as client details, financial records, and proprietary business information.

4. Privilege Escalation: If an attacker gains access to accounts with higher privileges, they can escalate their actions, leading to further compromise of the application's data and functionalities.

5. Regulatory Compliance Issues: Failure to protect user passwords adequately can lead to non-compliance with data protection regulations, resulting in fines and legal actions.

The presence of the CWE-759 vulnerability allows an attacker to severely compromise the confidentiality of **Caterease**, jeopardizing user and client data. Remediation of this vulnerability is essential to mitigate these risks and safeguard both clients and users from potential harm.

End of Risk Summary

CVE-2024-38882 - OVERVIEW

CWE-78

CVE-2024-38882: An issue in Horizon Business Services Inc. Caterease allows a remote attacker to perform command line execution through SQL Injection due to improper neutralization of special elements used in an OS command.

Vulnerability Type: CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

Vendor of the Product: Horizon Business Services Inc.
Affected Product: Caterease
Affected Versions: 16.0.1.1663 through 24.0.1.2405

Attack Vector: Remote
Attack Type: CAPEC-108: Command Line Execution through SQL Injection

Vulnerability Summary: Caterease is vulnerable to remote code execution through SQL Injection. The improper neutralization of special elements in SQL commands allows attackers to inject and execute arbitrary commands on the SQL server via xp_cmdshell. By exploiting this vulnerability, an attacker can craft malicious SQL queries that are executed with high-level privileges, enabling them to perform unauthorized actions on the server. This includes reading or modifying sensitive data, creating or deleting database objects, and even executing system-level commands.

The ability to execute arbitrary commands can lead to unauthorized access to the SQL server, allowing the attacker to manipulate data, disrupt operations, and compromise the entire system. This vulnerability severely impacts the server's confidentiality by exposing sensitive information, the integrity by allowing unauthorized data modifications, and the availability by enabling actions that can disrupt or disable the server. Furthermore, the exploit can serve as a foothold for further attacks within the network, escalating the overall security risk.

CVSS Base Score: Critical Risk - 9.6
CVSS v3.1 Vector: AV:A/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

Exploitability Metrics:
Attack Vector (AV): Adjacent Network
Attack Complexity (AC): Low
Privileges Required (PR): None
User Interaction (UI): None
Scope (S): Changed

Impact Metrics:
Confidentiality (C): High
Integrity (I): High
Availability (A): High

End of Overview

CVE-2024-38882 - IMPACT

CWE-78

Confidentiality: HIGH

The CWE-78 vulnerability, involving the improper neutralization of special elements used in an OS command injection, poses a significant risk to confidentiality, warranting a high severity rating. Exploiting this vulnerability allows an attacker to gain unauthorized access to sensitive data stored on the SQL server. Once exploited, an attacker can read confidential information, including user data, client records, and proprietary business information, compromising the confidentiality of the database.

Integrity: HIGH

The CWE-78 vulnerability, involving the improper neutralization of special elements used in an OS command injection, poses a significant risk to integrity, warranting a high severity rating. Exploiting this vulnerability allows an attacker to modify the data stored on the SQL server. Once exploited, an attacker can alter, insert, or delete critical data, leading to data corruption, loss of data integrity, and potential operational disruptions.

Availability: HIGH

The CWE-78 vulnerability, involving the improper neutralization of special elements used in an OS command injection, poses a significant risk to availability, warranting a high severity rating. Exploiting this vulnerability allows an attacker to execute unauthorized commands on the SQL server. Once exploited, an attacker can run arbitrary commands, potentially disrupting the availability of services by shutting down the server, deleting data, or overloading the system with resource-intensive operations.

End of Impact Statements

CVE-2024-38882 - RISK SUMMARY

CWE-78

The improper neutralization of special elements used in an OS command injection can lead to severe security risks, resulting in unauthorized access, data manipulation, and system disruption. Once an attacker exploits the vulnerability, they can perform the following actions. These actions include, but are not limited to:

1. Data Exfiltration: The attacker can read and export sensitive data from the server, including personal information, financial records, proprietary business information, and other critical data stored on the server.

2. Privilege Escalation: The attacker can escalate their privileges to gain administrative or root access on the server, allowing them to modify user permissions, access sensitive system files, and perform administrative actions.

3. Service Disruption: The attacker can disrupt services by overwhelming the server with requests, shutting down critical services, or causing other conditions that lead to service outages and operational disruptions.

4. System Manipulation: The attacker can install malware, create backdoors, and modify system files and configurations on the server, potentially compromising system integrity, security, and operational stability.

5. Network Exploitation: The attacker can use the compromised server as a pivot point to move laterally within the network, compromising other systems and capturing network traffic for further exploitation.

6. Compliance Violations: The organization may face fines, sanctions, and legal actions due to non-compliance with data protection regulations if the breach involves personal data, leading to financial and reputational damage.

The presence of the CWE-78 vulnerability allows an attacker to severely compromise the confidentiality, integrity, and availability of **Caterease**, jeopardizing sensitive user and client data. Remediation of this vulnerability is essential to mitigate these risks and safeguard both the clients and users from potential harm.

End of Risk Summary

CVE-2024-38883 - OVERVIEW

CWE-757

CVE-2024-38883: An issue in Horizon Business Services Inc. Caterease allows a remote attacker to perform a Drop Encryption Level attack due to the selection of a less-secure algorithm during negotiation.

Vulnerability Type: CWE-757: Selection of Less-Secure Algorithm During Negotiation ('Algorithm Downgrade')

Vendor of the Product: Horizon Business Services Inc.
Affected Product: Caterease
Affected Versions: 16.0.1.1663 through 24.0.1.2405

Attack Vector: Remote
Attack Type: CAPEC-620: Drop Encryption Level

Vulnerability Summary: Caterease does not enforce encryption during the TDS7 PreLogin authentication sequence, making it susceptible to a downgrade attack. Attackers can intercept the initial handshake between the Caterease client and the SQL server and manipulate the server's response to indicate that encryption is not supported. As a result, the client will proceed to send sensitive information, including database credentials, in plaintext over the network.

By exploiting this vulnerability, attackers can capture the unencrypted credentials and use them to gain unauthorized access to the SQL database. This exposure not only compromises the confidentiality of the credentials but also allows attackers to read, modify, or delete database records, leading to significant data breaches and integrity issues.

CVSS Base Score: Critical Risk - 9.3
CVSS v3.1 Vector: AV:A/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:N

Exploitability Metrics:
Attack Vector (AV): Adjacent Network
Attack Complexity (AC): Low
Privileges Required (PR): None
User Interaction (UI): None
Scope (S): Changed

Impact Metrics:
Confidentiality (C): High
Integrity (I): High
Availability (A): None

End of Overview

CVE-2024-38883 - IMPACT

CWE-757

Confidentiality: HIGH

The CWE-757 vulnerability, involving the selection of a less-secure algorithm during negotiation, poses a significant risk to confidentiality, warranting a high severity rating. Exploiting this vulnerability allows an attacker to downgrade the encryption level and intercept sensitive data during transmission. Once exploited, an attacker can read confidential information, including database credentials, compromising the confidentiality of the database.

Integrity: HIGH

The CWE-757 vulnerability, involving the selection of a less-secure algorithm during negotiation, poses a significant risk to integrity, warranting a high severity rating. Exploiting this vulnerability allows an attacker to manipulate data during transmission. Once exploited, an attacker can alter the data being transmitted between the client and the server, leading to data corruption and loss of data integrity.

End of Impact Statements

CVE-2024-38883 - RISK SUMMARY

CWE-757

The selection of a less-secure algorithm during negotiation can lead to severe security risks, resulting in unauthorized access and data manipulation. Once an attacker exploits the vulnerability, they can perform the following actions. These actions include, but are not limited to:

1. Credential Theft: An attacker can intercept the cleartext transmission of SQL user credentials during the handshake process, leading to unauthorized access to the SQL database.

2. Session Hijacking: The attacker can hijack the session between the client and server, allowing them to inject malicious commands, alter data, or disrupt services.

3. Increased Attack Surface: With communication left unencrypted, the attacker has more opportunities to discover and exploit other vulnerabilities within the application or database.

4. Data Exfiltration: With the rest of the communication left unencrypted, the attacker can continue to intercept sensitive data transmitted between the client and server, including client details, financial records, and proprietary business information.

5. Data Manipulation: The attacker can modify the data being transmitted between the client and server, leading to data corruption and integrity issues within the SQL database.

6. Compliance Violations: Failure to protect sensitive data in transit can lead to non-compliance with data protection regulations, resulting in fines and legal actions.

The presence of the CWE-757 vulnerability allows an attacker to severely compromise the confidentiality and integrity of **Caterease**, jeopardizing sensitive data. Remediation of this vulnerability is essential to mitigate these risks and safeguard both clients and users from potential harm.

End of Risk Summary

CVE-2024-38884 - OVERVIEW

CWE-358

CVE-2024-38884: An issue in Horizon Business Services Inc. Caterease allows a local attacker to perform an Authentication Bypass attack due to improperly implemented security checks for standard authentication mechanisms.

Vulnerability Type: CWE-358: Improperly Implemented Security Check for Standard

Vendor of the Product: Horizon Business Services Inc.
Affected Product: Caterease
Affected Versions: 16.0.1.1663 through 24.0.1.2405

Attack Vector: Local
Attack Type: CAPEC-115: Authentication Bypass

Vulnerability Summary: Caterease's Active Directory authentication mechanism has improperly implemented security checks, allowing local attackers to bypass authentication. Instead of performing a robust verification with the Active Directory Domain Controller, the application merely checks if the profile name of the local user matches the Active Directory username set for the Caterease user account. As a result, attackers with the ability to create local profiles can exploit this flaw by creating a local user with the same profile name as any valid Active Directory user.

This vulnerability enables attackers to gain unauthorized access to Caterease user accounts that have Active Directory authentication enabled. By logging in with a locally created profile that matches an Active Directory user, attackers can bypass the need for valid Active Directory credentials. This leads to significant security risks, including data breaches, unauthorized data access, and data manipulation.The improper implementation of security checks in the Active Directory authentication mechanism compromises both the confidentiality and integrity of the application.

CVSS Base Score: High Risk - 7.7
CVSS v3.1 Vector: AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:NA

Exploitability Metrics:
Attack Vector (AV): Local
Attack Complexity (AC): Low
Privileges Required (PR): None
User Interaction (UI): None
Scope (S): Unchanged

Impact Metrics:
Confidentiality (C): High
Integrity (I): High
Availability (A): None

End of Overview

CVE-2024-38884 - IMPACT

CWE-358

Confidentiality: HIGH

The CWE-358 vulnerability, involving improperly implemented security checks for standard authentication mechanisms, poses a significant risk to confidentiality, warranting a high severity rating. Exploiting this vulnerability allows an attacker to bypass authentication and gain unauthorized access to sensitive data. Once exploited, an attacker can read confidential information, including user data and client records, compromising the confidentiality of the account.

Integrity: HIGH

The CWE-358 vulnerability, involving improperly implemented security checks for standard authentication mechanisms, poses a significant risk to integrity, warranting a high severity rating. Exploiting this vulnerability allows an attacker to modify data within the application. Once exploited, an attacker can alter, insert, or delete critical data, leading to data corruption and loss of data integrity.

End of Impact Statements

CVE-2024-38884 - RISK SUMMARY

CWE-358

Improperly implemented security checks for standard authentication mechanisms can lead to severe security risks, resulting in unauthorized access and data manipulation. Once an attacker exploits the vulnerability, they can perform the following actions. These actions include, but are not limited to:

1. Account Takeover: An attacker can create a local user profile with the same name as an Active Directory user, allowing them to log in to **Caterease** as that user and take over the account.

2. Unauthorized Access: This vulnerability allows unauthorized users to gain access to the **Caterease** application without needing valid Active Directory credentials, bypassing intended security measures.

3. Privilege Escalation: If the attacker targets a **Caterease** user with higher privileges, they can escalate their own privileges within the **Caterease** application, gaining access to sensitive functionalities and data.

4. Data Breach: The attacker can access sensitive data associated with the impersonated user, including client details, financial records, and proprietary business information, leading to data breaches.

5. Data Manipulation: Once logged in as another user, the attacker can alter, insert, or delete data within the **Caterease** application, leading to data corruption and integrity issues.

6. Loss of Accountability: Logging in as another user without proper authentication disrupts audit trails and accountability, making it difficult to track actions back to the actual perpetrator.

7. Internal Threats: Employees or insiders with knowledge of this vulnerability can exploit it to gain unauthorized access to information and systems, increasing the risk of insider threats.

The presence of the CWE-358 vulnerability allows an attacker to severely compromise the confidentiality and integrity of **Caterease**, jeopardizing sensitive data. Remediation of this vulnerability is essential to mitigate these risks and safeguard both clients and users from potential harm.

End of Risk Summary

CVE-2024-38885 - OVERVIEW

CWE-259

CVE-2024-38885: An issue in Horizon Business Services Inc. Caterease allows a remote attacker to perform unauthorized access using known operating system credentials due to hardcoded SQL user credentials in the client application.

Vulnerability Type: CWE-259: Use of Hard-coded Password

Vendor of the Product: Horizon Business Services Inc.
Affected Product: Caterease
Affected Versions: 16.0.1.1663 through 24.0.1.2405

Attack Vector: Remote
Attack Type: CAPEC-653: Use of Known Operating System Credentials

Vulnerability Summary: Caterease contains hardcoded SQL user credentials within the client application. These credentials are embedded in the software and are identical across all instances of the application, making them a single point of failure. Attackers who gain access to the client application can easily extract these hardcoded credentials and use them to log in to any Caterease SQL database.

The SQL user associated with these credentials is a member of the DBO group, granting it elevated privileges within the SQL server. This means that once attackers have the credentials, they can access and control the entire SQL server. They can read and exfiltrate sensitive data, modify or delete database records, and execute arbitrary SQL commands.This vulnerability severely impacts the confidentiality, integrity, and availability of the database.

CVSS Base Score: High Risk - 8.8
CVSS v3.1 Vector: AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Exploitability Metrics:
Attack Vector (AV): Adjacent Network
Attack Complexity (AC): Low
Privileges Required (PR): None
User Interaction (UI): None
Scope (S): Unchanged

Impact Metrics:
Confidentiality (C): High
Integrity (I): High
Availability (A): High

End of Overview

CVE-2024-38885 - IMPACT

CWE-259

Confidentiality: HIGH

The CWE-259 vulnerability, involving the use of hardcoded passwords, poses a significant risk to confidentiality, warranting a high severity rating. Exploiting this vulnerability allows an attacker to use the hardcoded credentials to gain unauthorized access to sensitive data stored on the SQL server. Once exploited, an attacker can read confidential information, including user data, client records, and proprietary business information, compromising the confidentiality of the database.

Integrity: HIGH

The CWE-259 vulnerability, involving the use of hardcoded passwords, poses a significant risk to integrity, warranting a high severity rating. Exploiting this vulnerability allows an attacker to use the hardcoded credentials to modify data stored on the SQL server. Once exploited, an attacker can alter, insert, or delete critical data, leading to data corruption, loss of data integrity, and potential operational disruptions.

Availability: HIGH

The CWE-259 vulnerability, involving the use of hardcoded passwords, poses a significant risk to availability, warranting a high severity rating. Exploiting this vulnerability allows an attacker to use the hardcoded credentials to execute unauthorized commands within the SQL database. Once exploited, an attacker can run arbitrary SQL commands, potentially disrupting the availability of the database services by deleting data, altering database structures, or executing resource-intensive operations that degrade performance.

End of Impact Statements

CVE-2024-38885 - RISK SUMMARY

CWE-259

The use of hardcoded passwords can lead to severe security risks, resulting in unauthorized access, data manipulation, and disruption within the SQL database. Once an attacker exploits the vulnerability, they can perform the following actions. These actions include, but are not limited to:

1. Credential Theft: Attackers can extract the hard-coded credentials from the client application, gaining unauthorized access to the SQL database.

2. Unauthorized Access: With the hard-coded credentials, attackers can access the SQL database without needing to bypass any authentication mechanisms, leading to unauthorized access to sensitive data.

3. Data Exfiltration: Attackers can use the hard-coded credentials to read and export sensitive data from the SQL database, including client details, financial records, and proprietary business information.

4. Privilege Escalation: If the hard-coded credentials have higher privileges, attackers can escalate their access within the SQL database, potentially compromising more sensitive data and functionalities.

5. Data Manipulation: Attackers can use the hard-coded credentials to alter, insert, or delete data within the SQL database, leading to data corruption and integrity issues.

6. System Compromise: Attackers can use the hard-coded credentials to execute SQL commands that may compromise the SQL server or other connected systems, leading to further exploitation.

7. Increased Attack Surface: The existence of a known set of credentials increases the attack surface, making it easier for attackers to target and compromise multiple installations of the software.

8. Compliance Violations: The use of hard-coded passwords can lead to non-compliance with data protection regulations, resulting in fines and legal actions.

The presence of the CWE-259 vulnerability allows an attacker to severely compromise the confidentiality, integrity, and availability of **Caterease** SQL database, jeopardizing sensitive user and client data. Remediation of this vulnerability is essential to mitigate these risks and safeguard both the clients and users from potential harm.

End of Risk Summary

CVE-2024-38886 - OVERVIEW

CWE-940

CVE-2024-38886: An issue in Horizon Business Services Inc. Caterease allows a remote attacker to perform a Traffic Injection attack due to improper verification of the source of a communication channel.

Vulnerability Type: CWE-940: Improper Verification of Source of a Communication Channel

Vendor of the Product: Horizon Business Services Inc.
Affected Product: Caterease
Affected Versions: 16.0.1.1663 through 24.0.1.2405

Attack Vector: Remote
Attack Type: CAPEC-594: Traffic Injection

Vulnerability Summary: Caterease lacks proper verification of the source of communication channels, making it susceptible to TCP packet injection attacks. This vulnerability arises because the application does not use encryption or other verification methods to ensure the authenticity of the packets being exchanged between the client and server. As a result, attackers on the same network can intercept the communication and inject arbitrary packets into the communication stream.

By exploiting this vulnerability, attackers can manipulate the data being transmitted between the client and server. They can alter, insert, or delete packets to disrupt the normal operation of the application, potentially leading to data corruption or loss. This vulnerability impacts the confidentiality, integrity, and availability of the application, as it allows attackers to intercept sensitive data, tamper with transmitted information, and disrupt service availability.

CVSS Base Score: High Risk - 8.8
CVSS v3.1 Vector: AV:A/AC:L/PR:N/UI:N/S:C/C:H/I:L/A:L

Exploitability Metrics:
Attack Vector (AV): Adjacent Network
Attack Complexity (AC): Low
Privileges Required (PR): None
User Interaction (UI): None
Scope (S): Changed

Impact Metrics:
Confidentiality (C): High
Integrity (I): Low
Availability (A): Low

End of Overview

CVE-2024-38886 - IMPACT

CWE-940

Confidentiality: HIGH

The CWE-940 vulnerability, involving the improper verification of the source of a communication channel, poses a significant risk to confidentiality, warranting a high severity rating. Exploiting this vulnerability allows an attacker to intercept and read data being transmitted between the **Caterease** client and the **Caterease** SQL/Application servers.Once exploited, an attacker can read confidential information, including user data, client records, and proprietary business information, compromising the confidentiality of the database.

Integrity: LOW

The CWE-940 vulnerability, involving improper verification of the source of a communication channel, poses a risk to integrity, warranting a low severity rating. Exploiting this vulnerability allows an attacker to inject malicious packets into the communication stream. Once exploited, an attacker can potentially alter the data being transmitted, leading to data corruption and loss of integrity.

Availability: LOW

The CWE-940 vulnerability, involving improper verification of the source of a communication channel, poses a risk to availability, warranting a low severity rating. Exploiting this vulnerability allows an attacker to inject packets that disrupt the communication stream. Once exploited, an attacker can cause service disruptions, resulting in decreased availability and potential denial of service.

End of Impact Statements

CVE-2024-38886 - RISK SUMMARY

CWE-259

Improper verification of the source of a communication channel can lead to security risks, resulting in data manipulation and service disruptions. Once an attacker exploits the vulnerability, they can perform the following actions. These actions include, but are not limited to:

1. Data Interception: An attacker can intercept and read data being transmitted between the client and server, leading to unauthorized access to sensitive information.

2. Data Manipulation: The attacker can modify the data in transit, leading to data corruption, integrity issues, and unauthorized alterations to the information being exchanged.

3. Session Hijacking: The attacker can take over an existing communication session between the client and server, potentially gaining unauthorized access to the application with the privileges of the intercepted session.

4. Command Injection: The attacker can inject malicious commands into the communication stream, causing the server or client to execute unintended and potentially harmful operations.

5. Service Disruption: The attacker can inject packets that disrupt the normal communication between the client and server, leading to denial of service or other operational disruptions.

6. Replay Attacks: The attacker can capture and replay packets, causing the server or client to perform actions multiple times, which can lead to unintended consequences or exploitation of application logic.

The presence of the CWE-940 vulnerability allows an attacker to compromise the confidentiality, integrity and availability of **Caterease**. Remediation of this vulnerability is essential to mitigate these risks and safeguard both clients and users from potential harm.

End of Risk Summary

CVE-2024-38887 - OVERVIEW

CWE-250

CVE-2024-38887: An issue in Horizon Business Services Inc. Caterease allows a remote attacker to expand control over the operating system from the database due to the execution of commands with unnecessary privileges.

Vulnerability Type: CWE-250: Execution with Unnecessary Privileges

Vendor of the Product: Horizon Business Services Inc.
Affected Product: Caterease
Affected Versions: 16.0.1.1663 through 24.0.1.2405

Attack Vector: Remote
Attack Type: CAPEC-470: Expanding Control over the Operating System from the Database

Vulnerability Summary: Caterease grants excessive privileges to the default Caterease SQL user by making this user a member of the dbo role in the SQL database. This role grants full administrative access not only to the Caterease database but also to all other databases within the SQL server. This misconfiguration means that any action performed by the Caterease client, regardless of the actual user's privileges within the application, is executed with administrative-level permissions in the SQL database.

Exploiting this vulnerability, attackers can execute unauthorized commands with full administrative rights, leading to unauthorized access to sensitive data, data manipulation, and potential system compromise. Attackers can read, modify, or delete critical data, create new users with elevated privileges, and execute arbitrary SQL commands, which can disrupt database operations. This severely impacts the confidentiality, integrity, and availability of the SQL server and its databases, making it imperative to remediate this vulnerability by properly configuring user roles and privileges.

CVSS Base Score: Critical Risk - 9.6
CVSS v3.1 Vector: AV:A/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

Exploitability Metrics:
Attack Vector (AV): Adjacent Network
Attack Complexity (AC): Low
Privileges Required (PR): Low
User Interaction (UI): None
Scope (S): Changed

Impact Metrics:
Confidentiality (C): High
Integrity (I): High
Availability (A): High

End of Overview

CVE-2024-38887 - IMPACT

CWE-250

Confidentiality: HIGH

The CWE-250 vulnerability, involving the execution of commands with unnecessary privileges, poses a significant risk to confidentiality, warranting a high severity rating. Exploiting this vulnerability allows an attacker to gain unauthorized access to sensitive data stored on the SQL server. Once exploited, an attacker can read confidential information, including user data, client records, and proprietary business information, compromising the confidentiality of the database.

Integrity: HIGH

The CWE-250 vulnerability, involving the execution of commands with unnecessary privileges, poses a significant risk to integrity, warranting a high severity rating. Exploiting this vulnerability allows an attacker to modify data stored on the SQL server. Once exploited, an attacker can alter, insert, or delete critical data, leading to data corruption, loss of data integrity, and potential operational disruptions.

Availability: HIGH

The CWE-250 vulnerability, involving the execution of commands with unnecessary privileges, poses a significant risk to availability, warranting a high severity rating. Exploiting this vulnerability allows an attacker to execute unauthorized commands on the SQL database and server. Once exploited, an attacker can run arbitrary commands, potentially disrupting the availability of the database services by shutting down the server, deleting data, or overloading the system with resource-intensive operations.

End of Impact Statements

CVE-2024-38887 - RISK SUMMARY

CWE-250

The execution of commands with unnecessary privileges can lead to severe security risks, resulting in unauthorized access, data manipulation, and system disruption. Once an attacker exploits the vulnerability, they can perform the following actions. These actions include, but are not limited to:

1. Data Exfiltration: An attacker can extract sensitive data from the SQL database, including personal information, financial records, and proprietary business information, due to the elevated privileges.

2. Data Manipulation: The attacker can alter, insert, or delete data within the SQL database, leading to data corruption and integrity issues.

3. Privilege Escalation: Even users with minimal application-level permissions can perform high-privilege actions on the SQL database, leading to unintended privilege escalation.

4. Database Compromise: The attacker can exploit the excessive privileges granted to the **Caterease** SQL user, compromising not only the **Caterease** SQL database but also any other databases hosted on the same SQL server.

5. Execution of Arbitrary Commands: The attacker can execute arbitrary SQL commands, potentially enabling further attacks, such as the creation of new database users, granting additional privileges, or dropping critical database tables.

6. Service Disruption: The attacker can disrupt database services by executing commands that impact the availability and performance of the SQL database, such as locking tables, terminating connections, or overloading the system.

7. Backdoor Installation: The attacker can create backdoors within the SQL database by creating new users with high privileges or installing malicious triggers and stored procedures.

The presence of the CWE-250 vulnerability allows an attacker to severely compromise the confidentiality, integrity, and availability of **Caterease,** jeopardizing sensitive user and client data. Remediation of this vulnerability is essential to mitigate these risks and safeguard both the clients and users from potential harm.

End of Risk Summary

CVE-2024-38888 - OVERVIEW

CWE-307

CVE-2024-38888: An issue in Horizon Business Services Inc. Caterease allows a local attacker to perform a Password Brute Forcing attack due to improper restriction of excessive authentication attempts.

Vulnerability Type: CWE-307: Improper Restriction of Excessive Authentication Attempts

Vendor of the Product: Horizon Business Services Inc.
Affected Product: Caterease
Affected Versions: 16.0.1.1663 through 24.0.1.2405

Attack Vector: Local
Attack Type: CAPEC-49: Password Brute Forcing

Vulnerability Summary: Caterease lacks adequate controls to prevent excessive authentication attempts, making it susceptible to brute force attacks. The login mechanism in Caterease activates the "OK" button only when a correct password is entered, allowing attackers to test passwords without actually sending them to the server. This design flaw enables attackers to systematically try numerous password combinations until they find the correct one, effectively bypassing standard security measures that should limit failed login attempts.

By exploiting this vulnerability, attackers can eventually gain unauthorized access to user accounts, leading to significant security risks. Unauthorized access allows attackers to compromise the confidentiality of user data and perform actions within the application that may compromise data integrity.

CVSS Base Score: Medium Risk - 6.8
CVSS v3.1 Vector: AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:N

Exploitability Metrics:
Attack Vector (AV): Local
Attack Complexity (AC): Low
Privileges Required (PR): None
User Interaction (UI): None
Scope (S): Unchanged

Impact Metrics:
Confidentiality (C): High
Integrity (I): Low
Availability (A): None

End of Overview

CVE-2024-38888 - IMPACT

CWE-307

Confidentiality: HIGH

The CWE-307 vulnerability, involving the improper restriction of excessive authentication attempts, poses a significant risk to confidentiality, warranting a high severity rating. Exploiting this vulnerability allows an attacker to gain unauthorized access to sensitive user data by brute-forcing passwords. Once exploited, an attacker can read confidential information, including user credentials and personal data, compromising the confidentiality of user accounts.

Integrity: LOW

The CWE-307 vulnerability, involving the improper restriction of excessive authentication attempts, poses a risk to integrity, warranting a low severity rating. Exploiting this vulnerability allows an attacker to gain unauthorized access to user accounts and potentially modify data. Once exploited, an attacker can alter user-related data, leading to data integrity issues, though this impact is less severe compared to the confidentiality risk.

End of Impact Statements

CVE-2024-38888 - RISK SUMMARY

CWE-307

Improper restriction of excessive authentication attempts can lead to security risks, primarily affecting the confidentiality and, to a lesser extent, the integrity of user accounts. Once an attacker exploits the vulnerability, they can perform the following actions. These actions include, but are not limited to:

1. Undetected Attacks: The lack of server-side logging for failed password attempts means that attacks can go undetected, allowing attackers to continue their efforts without alerting security teams.

2. Brute Force Attacks: Attackers can systematically try a large number of passwords to find the correct one without any restriction, leading to unauthorized access to user accounts.

3. Account Takeover: Successful brute force attacks can result in attackers gaining control of user accounts, potentially leading to misuse of account privileges.

4. Privilege Escalation: Compromised accounts, especially those with higher privileges, can be used to perform unauthorized actions within the application, leading to privilege escalation.

5. Data Breach: Once an account is compromised, attackers can access sensitive data associated with that account, including personal information, financial records, and proprietary business information.

6. Loss of Confidentiality: The ability to discover correct passwords without detection compromises the confidentiality of user credentials and associated data.

7. Integrity Issues: Attackers with access to user accounts can alter, insert, or delete data within the application, leading to data corruption and integrity issues.

The presence of the CWE-307 vulnerability allows an attacker to compromise the confidentiality and integrity of **Caterease** user accounts. Remediation of this vulnerability is essential to mitigate these risks and safeguard user data from potential harm.

End of Risk Summary

CVE-2024-38889 - OVERVIEW

CWE-89

CVE-2024-38889: An issue in Horizon Business Services Inc. Caterease allows a remote attacker to perform SQL Injection due to improper neutralization of special elements used in an SQL command.

Vulnerability Type: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

Vendor of the Product: Horizon Business Services Inc.
Affected Product: Caterease
Affected Versions: 16.0.1.1663 through 24.0.1.2405

Attack Vector: Remote
Attack Type: CAPEC-66: SQL Injection \ CAPEC-594: Traffic Injection

Vulnerability Summary: Caterease is vulnerable to SQL Injection due to improper neutralization of special elements in SQL commands. This vulnerability allows attackers to exploit the software by injecting malicious SQL queries through TCP packet injection techniques. Attackers can craft custom TDS payloads that bypass normal input validation and execute arbitrary SQL commands on the database.

By exploiting this vulnerability, attackers can gain unauthorized access to the SQL database, manipulate or delete data, and disrupt database services. This can lead to significant security breaches, including the exposure of sensitive information, unauthorized data modification, and denial of service. The ability to execute arbitrary SQL commands compromises the confidentiality, integrity, and availability of the SQL database.

CVSS Base Score: Critical Risk - 9.6
CVSS v3.1 Vector: AV:A/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

Exploitability Metrics:
Attack Vector (AV): Adjacent Network
Attack Complexity (AC): Low
Privileges Required (PR): None
User Interaction (UI): None
Scope (S): Changed

Impact Metrics:
Confidentiality (C): High
Integrity (I): High
Availability (A): High

End of Overview

CVE-2024-38889 - IMPACT

CWE-89

Confidentiality: HIGH

The CWE-89 vulnerability, involving the improper neutralization of special elements used in an SQL command, poses a significant risk to confidentiality, warranting a high severity rating. Exploiting this vulnerability allows an attacker to execute SQL queries that read sensitive data from the database. Once exploited, an attacker can access confidential information, including user data, client records, and proprietary business information, compromising the confidentiality of the database.

Integrity: HIGH

The CWE-89 vulnerability, involving the improper neutralization of special elements used in an SQL command, poses a significant risk to integrity, warranting a high severity rating. Exploiting this vulnerability allows an attacker to execute SQL queries that modify data within the database. Once exploited, an attacker can alter, insert, or delete critical data, leading to data corruption, loss of data integrity, and potential operational disruptions.

Availability: HIGH

The CWE-89 vulnerability, involving the improper neutralization of special elements used in an SQL command, poses a significant risk to availability, warranting a high severity rating. Exploiting this vulnerability allows an attacker to execute SQL queries that can disrupt the database services. Once exploited, an attacker can run commands that shut down the database, delete data, or overload the system, impacting the availability of the database services.

End of Impact Statements

CVE-2024-38889 - RISK SUMMARY

CWE-89

The improper neutralization of special elements used in an SQL command can lead to severe security risks, resulting in unauthorized access, data manipulation, and service disruption within the SQL database. Once an attacker exploits the vulnerability, they can perform the following actions. These actions include, but are not limited to:

1. Data Exfiltration: Attackers can execute SQL queries that extract sensitive data from the SQL database, including personal information, financial records, and proprietary business information.

2. Data Manipulation: Attackers can alter, insert, or delete data within the SQL database, leading to data corruption and integrity issues.

3. Privilege Escalation: Attackers can exploit SQL injection to gain elevated privileges within the database, potentially gaining administrative access and control over the database.

4. Authentication Bypass: Attackers can use SQL injection to bypass authentication mechanisms, allowing unauthorized access to the application and its data.

5. Database Compromise: Attackers can compromise the entire SQL database, affecting the integrity and availability of data and potentially leading to further exploits.

6. Denial of Service (DoS): Attackers can execute SQL queries that consume excessive resources, leading to performance degradation or complete denial of service for the SQL database.

The presence of the CWE-89 vulnerability allows an attacker to severely compromise the confidentiality, integrity, and availability of the **Caterease** SQL database, jeopardizing sensitive user and client data. Remediation of this vulnerability is essential to mitigate these risks and safeguard both the clients and users from potential harm.

End of Risk Summary

CVE-2024-38890 - OVERVIEW

CWE-294

CVE-2024-38890: An issue in Horizon Business Services Inc. Caterease allows a local attacker to perform an Authentication Bypass attack due to insufficient protection against capture-replay attacks.

Vulnerability Type: CWE-294: Authentication Bypass by Capture-replay

Vendor of the Product: Horizon Business Services Inc.
Affected Product: Caterease
Affected Versions: 16.0.1.1663 through 24.0.1.2405

Attack Vector: Local
Attack Type: CAPEC-115: Authentication Bypass

Vulnerability Summary: Caterease is vulnerable to authentication bypass through a capture-replay attack. This vulnerability arises because the application relies on the UID for authentication without proper session validation. A local attacker can exploit this by capturing the authentication request sent by the client and modifying the UID within the request. By replaying the modified request, the attacker can impersonate any user whose UID is known or can be guessed, gaining unauthorized access to their account.

This vulnerability allows attackers to bypass the authentication process and access the application as another user without needing their credentials. Once inside, the attacker can access sensitive information, perform unauthorized actions, and manipulate data. This severely compromises the confidentiality and integrity of user accounts, as it enables unauthorized access and potential data breaches.

CVSS Base Score: High Risk - 7.3
CVSS v3.1 Vector: AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:L

Exploitability Metrics:
Attack Vector (AV): Local
Attack Complexity (AC): Low
Privileges Required (PR): Low
User Interaction (UI): None
Scope (S): Unchanged

Impact Metrics:
Confidentiality (C): High
Integrity (I): High
Availability (A): Low

End of Overview

CVE-2024-38890 - IMPACT

CWE-294

Confidentiality: HIGH

The CWE-294 vulnerability, involving authentication bypass by capture-replay, poses a significant risk to confidentiality, warranting a high severity rating. Exploiting this vulnerability allows an attacker to bypass authentication and gain unauthorized access to another users account. Once exploited, an attacker can read confidential information, including user data and client records, compromising the confidentiality of the database.

Integrity: HIGH

The CWE-294 vulnerability, involving authentication bypass by capture-replay, poses a significant risk to integrity, warranting a high severity rating. Exploiting this vulnerability allows an attacker to bypass authentication and modify data within the application as a different user. Once exploited, an attacker can alter, insert, or delete critical data, leading to data corruption and loss of data integrity.

Availability: LOW

The CWE-294 vulnerability, involving authentication bypass by capture-replay, poses a risk to availability, warranting a low severity rating. Exploiting this vulnerability allows an attacker to bypass authentication and potentially execute unauthorized commands as another user. Once exploited, an attacker can perform actions that impact the availability of the application, though this impact is less severe compared to the confidentiality and integrity risks.

End of Impact Statements

CVE-2024-38890 - RISK SUMMARY

CWE-294

Authentication bypass by capture-replay can lead to security risks, primarily affecting the confidentiality and integrity of user accounts. Once an attacker exploits the vulnerability, they can perform the following actions. These actions include, but are not limited to:

1. Account Takeover: Attackers can log in as any user by modifying the UID in the captured authentication request, leading to unauthorized access to user accounts.

2. Privilege Escalation: Attackers can gain access to accounts with higher privileges, allowing them to perform administrative actions and access sensitive areas of the application.

3. Loss of Accountability: The ability to log in as another user without proper authentication disrupts audit trails and accountability, making it difficult to track actions back to the actual perpetrator.

4. Internal Threats: Employees or insiders with knowledge of this vulnerability can exploit it to gain unauthorized access to information and systems, increasing the risk of insider threats.

5. Data Breach: Attackers can access sensitive data associated with the compromised accounts, including personal information, financial records, and proprietary business information.

6. Data Manipulation: Once logged in as another user, attackers can alter, insert, or delete data within the application, leading to data corruption and integrity issues.

The presence of the CWE-294 vulnerability allows an attacker to severely compromise the confidentiality and integrity of **Caterease**, jeopardizing sensitive user and client data. Remediation of this vulnerability is essential to mitigate these risks and safeguard both the clients and users from potential harm.

End of Risk Summary

CVE-2024-38891 - OVERVIEW

CWE-319

CVE-2024-38891: An issue in Horizon Business Services Inc. Caterease allows a remote attacker to perform a Sniffing Network Traffic attack due to the cleartext transmission of sensitive information.

Vulnerability Type: CWE-319: Cleartext Transmission of Sensitive Information

Vendor of the Product: Horizon Business Services Inc.
Affected Product: Caterease
Affected Versions: 16.0.1.1663 through 24.0.1.2405

Attack Vector: Remote
Attack Type: CAPEC-158: Sniffing Network Traffic

Vulnerability Summary: Caterease leaks sensitive information, including user details, client details, database details, and software license keys, in cleartext during the application's startup phase. This vulnerability arises because the application transmits this information without encryption, making it vulnerable to interception by attackers using network sniffing tools. The lack of encryption during data transmission severely compromises the confidentiality of the transmitted information.

CVSS Base Score: High Risk - 7.4
CVSS v3.1 Vector: AV:A/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N

Exploitability Metrics:
Attack Vector (AV): Adjacent Network
Attack Complexity (AC): Low
Privileges Required (PR): None
User Interaction (UI): None
Scope (S): Changed

Impact Metrics:
Confidentiality (C): High
Integrity (I): None
Availability (A): None

End of Overview

CVE-2024-38891 - IMPACT

CWE-319

Confidentiality: HIGH

The CWE-319 vulnerability, involving the cleartext transmission of sensitive information, poses a significant risk to confidentiality, warranting a high severity rating. Exploiting this vulnerability allows an attacker to intercept and read sensitive data transmitted during the application's startup phase. Once exploited, an attacker can access confidential information, including user credentials, license keys, database details, and client information, compromising the confidentiality of the transmitted data.

End of Impact Statements

CVE-2024-38891 - RISK SUMMARY

CWE-319

The cleartext transmission of sensitive information can lead to severe security risks, resulting in unauthorized access to sensitive data. Once an attacker exploits the vulnerability, they can perform the following actions. These actions include, but are not limited to:

1. Data Interception: The attacker can intercept and read data transmitted in cleartext between the **Caterease** client and server. This intercepted data can include sensitive information such as user credentials, license keys, database details, and client details, leading to unauthorized access and potential misuse of this information.

2. Network Exploitation: By intercepting unencrypted data, the attacker can gain valuable insights into the network's communication patterns and database architecture. This information can be used to identify and exploit other vulnerabilities within the network, potentially leading to a broader compromise of the network infrastructure and systems.

3. Software Piracy: The attacker can intercept license keys transmitted in cleartext and use them to create unauthorized copies of the software. This can lead to significant financial losses for the software vendor due to illegal distribution and use of the software, as well as potential legal and reputational damage.

The presence of the CWE-319 vulnerability allows an attacker to severely compromise the confidentiality of **Caterease**, jeopardizing sensitive user and client data. Remediation of this vulnerability is essential to mitigate these risks and safeguard both the clients and users from potential harm.

End of Risk Summary

MITIGATIONS

Disclaimer: We would like to highlight that the mitigation methods provided over the next few pages are temporary workarounds that we have identified to address the specific attack vectors discussed in this report. However, it is important to note that these measures should not be interpreted as permanent or production-ready solutions. Implementation of these mitigation steps may have lasting side effects and may not be suitable for every use case or environment. We cannot guarantee their effectiveness or compatibility in all scenarios.

CVE-2024-38884: The Active Directory feature in **Caterease** allows users to be automatically logged into the application if their Active Directory username matches the profile name. However, no actual authentication is performed against the Active Directory domain controller. This means that anyone with the ability to create a local user profile can impersonate an Active Directory user by creating a local profile with the same name.

Mitigation: Remove the Active Directory feature from all **Caterease** user accounts to prevent its use for authentication. This will ensure that only valid authentication methods are used, thereby eliminating the vulnerability caused by improper security checks.

CVE-2024-38882: Caterease uses a default SQL user "Caterease" which is part of the DBO (Database Owner) role. This gives the user full administrative privileges, including the ability to enable xp_cmdshell, a stored procedure that allows execution of shell commands directly from SQL Server. This can be exploited by attackers to execute arbitrary commands on the server.

Mitigation: Remove the default SQL user "Caterease" from the DBO role and assign custom privileges that restrict operations to the confines of the **Caterease** database. This prevents the user from enabling xp_cmdshell and running commands outside the database, reducing the risk of arbitrary command execution.

CVE-2024-38887: The default SQL user "Caterease" in **Caterease** has excessive privileges as part of the DBO role, granting full access to all databases within the SQL server. This allows any command executed by the client application to run with administrative privileges, leading to unauthorized access and manipulation of data across all databases.

Mitigation: Remove the default SQL user "Caterease" from the DBO role and assign custom privileges that restrict operations to the confines of the **Caterease** database. This measure limits the user's privileges and mitigates the risk of unauthorized command execution and privilege escalation.

Continued on Next Page

MITIGATIONS CONTINUED

CVE-2024-38885: Caterease uses hard-coded SQL credentials within the client application for connecting to the SQL database. These credentials are the same across all installations of **Caterease,** making them easily exploitable if discovered.

Workaround: Segregate the **Caterease** SQL database from other critical databases and systems to limit the potential impact of a compromised hard-coded password. Additionally, disable the SQL Browser option to prevent remote login attempts using the hard-coded credentials. This adds an additional layer of security, making it harder for attackers to exploit the vulnerability remotely.

CVE-2024-38881: Caterease stores user password hashes without incorporating a salt. Salts are random values added to passwords before hashing to ensure that identical passwords do not result in the same hash. Without salts, the hashes are vulnerable to rainbow table attacks, where precomputed hash values for common passwords are used to crack them.

Workaround: Encourage users to create complex, unique **Caterease** passwords that are not part of standard word lists and are not reused across other applications. This approach reduces the effectiveness of rainbow table attacks and helps protect user accounts from unauthorized access.

CVE-2024-38888: The **Caterease** login screen activates the "OK" button only when a correct password is entered. This allows attackers to determine if a password is correct without sending it to the server, facilitating unlimited password attempts without detection.

Workaround: Encourage users to create complex, unique **Caterease** passwords that are not part of standard word lists and are not reused across other applications. Strong, unique passwords make brute force attacks more difficult.

End of Mitigations

ENCRYPTION ISSUES

Several vulnerabilities in **Caterease** stem from the lack of enforced encryption during the TDS Pre-Login sequence. These vulnerabilities include:

1. CVE-2024-38883: TDS7 Client Downgrade
2. CVE-2024-38886: TCP Packet Injection
3. CVE-2024-38889: SQL Injection
4. CVE-2024-38890: Authentication Bypass by Capture-replay
5. CVE-2024-38891: Cleartext Transmission of Sensitive Information

The **Caterease** Client Application does not enforce encryption when initiating the TDS Pre-Login request. As a result, attackers can intercept and modify the server response to downgrade the encryption level, exposing the SQL user credentials and leaving subsequent communications unencrypted.

This allows attackers to perform various attacks, including downgrades, packet injections, SQL injections, authentication bypasses, and intercepting cleartext sensitive information.

Mitigation Note: While forcing encryption from the server side can help, it does not fully mitigate the risk. If the client does not enforce encryption, an attacker can perform a man-in-the-middle (MITM) attack where the communication between the client and the attacker remains unencrypted. The server-side encryption does not protect the initial communication between the client and the attacker, leaving ALL vulnerabilities still exploitable.

Due to the lack of official fixes from **Horizon Business Services**, we have outlined best practices and specific methods that could potentially reduce the risks associated with these critical vulnerabilities in **Caterease**. These mitigations are meant to provide options to reduce attack vectors but should not be considered complete solutions.

The only definitive way to secure **Caterease** is for **Horizon Business Services** to address these vulnerabilities through official patches and updates. We strongly urge the vendor to take prompt action in releasing fixes to protect their users. Additionally, we recommend that the vendor conducts more rigorous internal security audits to prevent such vulnerabilities from being introduced in the first place and reaching end users.

Regular security assessments, updates, and audits are essential for both clients and software vendors to maintain the security of their systems. It is crucial for software vendors to continuously evaluate and secure their products to ensure the safety of their users, while users must remain vigilant and proactive in safeguarding their data and systems.

End of Encryption Issues