Honeywell

Security Notification
SN 2023-12-20 01

2023-12-20

Voice Console SN 2023-12-20 01 Blind SQL Injection

This article contains:

It applies to:

- Voice Console versions: v5.6.2 & v5.6.3

To mitigate the risk:

- Follow Resolution Description procedure.

Skills prerequisite:

Extensive Voice Console DB Knowledge.

Summary

This security notification informs users of Voice Console of a software vulnerability identified as CVE-2023-6589. Honeywell recommends that immediate steps be taken to ensure this potential vulnerability is mitigated and patch is installed on any production operating system.

Attention: .Due to the wide variety of security controls, implementations and interfaces, it is the responsibility of each customer to assess the potential impact within a specific operating environment.

Vulnerability Synopsis

CWE-200 Exposure of Sensitive Information to an Unauthorized Actor in the Voice Console Database in Voice Console Versions 5.6.2 & 5.6.3 on Windows, allows an attacker to gain access to sensitive information stored within the Voice Console Database. The vulnerability can be exploited via a specially crafted network request to the Voice Console system. This request bypasses the standard authentication mechanisms, allowing unauthorized access to the database.

CVSS Base Score: 7.5(High)

Temporal Score: 6.5 (Medium)

Affected Products

The vulnerability affects the following product versions:

- Voice Console versions: v5.6.2 & v5.6.3

CWE-200 Exposure of Sensitive Information to an Unauthorized Actor in the Voice Console Database in Voice Console Versions 5.6.2 & 5.6.3 on Windows, allows an attacker to gain access to sensitive information stored within the Voice Console Database. The vulnerability can be exploited via a specially crafted network request to the Voice Console system. This request bypasses the standard authentication mechanisms, allowing unauthorized access to the database.

Mitigation

Honeywell recommends that customers with affected products should take the following steps to protect themselves:

- Upgrade appropriate to v5.6.2.001 if currently running v5.6.2
- Upgrade appropriate to v5.6.3.001 if currently running v5.6.3

Resolution Description

Honeywell has released update packages for Voice Console versions 5.6.2 and 5.6.3.

The package can be downloaded by contacting Technical Support.

To install the update on any Voice Console Server:

1. Contact Technical Support to receive a link to Kiteworks
2. Download the Patch
3. Install the Patch per Tech Support instructions.

Prerequisites

- Appropriate Patch Files for your version of Voice Console.

Credit

Thanks to Christoph Van de Vondel, CaptureTech Belgium, for reporting this potential vulnerability.

Appendix: About CVSS

The Common Vulnerability Scoring System (CVSS) is an open standard for communicating the characteristics and severity of software vulnerabilities. The Base score represents the intrinsic qualities of a vulnerability. The Temporal score reflects the characteristics of a vulnerability that change over time. The Environmental score is an additional score that can be used by CVSS, but is not supplied as it will differ for each customer.

The Base score has a value ranging from 0 to 10. The Temporal score has the same range and is a modification of the Base score due to current temporary factors.

The severity of the score can be summarized as follows:

Severity Rating	CVSS Score
None	0.0
Low	0.1 – 3.9
Medium	4.0 – 6.9
High	7.0 – 8.9
Critical	9.0 – 10.0

A CVSS score is also represented as a vector string, a compressed textual representation of the values used to derive the score.

Detailed information about CVSS can be found at http://www.first.org/cvss.

DISCLAIMERS

- CUSTOMERS ARE RESPONSIBLE FOR ASSESSING THE IMPACT OF ANY ACTUAL OR POTENTIAL SECURITY VULNERABILITY.
- YOUR USE OF THE INFORMATION ON THIS DOCUMENT OR MATERIALS LINKED FROM THIS DOCUMENT IS AT YOUR OWN RISK.
- HONEYWELL RESERVES THE RIGHT TO CHANGE OR UPDATE THIS DOCUMENT AT ANY TIME AND WITHOUT NOTICE.
- HONEYWELL PROVIDES THE CVSS SCORES “AS IS” WITHOUT WARRANTY OF ANY KIND. HONEYWELL DISCLAIMS THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PURPOSE AND MAKES NO EXPRESS WARRANTIES EXCEPT AS MAY BE STATED IN A WRITTEN AGREEMENT WITH AND FOR ITS CUSTOMERS
- IN NO EVENT WILL HONEYWELL BE LIABLE TO ANYONE FOR ANY DIRECT, INDIRECT, SPECIAL, OR CONSEQUENTIAL DAMAGES.