The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE
www.cisa.gov/tlp
Information may be distributed without restriction, subject to standard copyright rules.

DATE(S) ISSUED:
03/02/2022

SUBJECT:
A Vulnerability in Mitel MiCollab and MiVoice Business Express Could Allow for Unauthorized Disclosure of Data

OVERVIEW:
A vulnerability has been discovered in Mitel MiCollab and MiVoice Business Express, which could allow for the unauthorized disclosure of data as well as result in denial of service.

- Mitel MiCollab is an enterprise collaboration software and tools platform solution that securely provides communications.
- MiVoice Business Express provides a complete communications solution for small to mid-range businesses.

Successful exploitation of this vulnerability could allow for unauthorized disclosure of data as well as result in denial of service. Depending on the goal of the attacker they could view sensitive information that should not be accessible, or create denial of service conditions within impacted the system.

THREAT INTELLIGENCE:
The MS-ISAC has been made aware that this vulnerability has been exploited in the wild.

SYSTEMS AFFECTED:

- Mitel MiCollab R9.4SP1 and earlier versions
- MiVoice Business Express R8.1 and earlier versions

RISK:

Government:

- Large and medium government entities: **High**

- Small government entities: **Medium**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **Medium**

Home users: Low

TECHNICAL SUMMARY:
A vulnerability has been discovered in Mitel MiCollab and MiVoice Business Express, which could allow for the unauthorized disclosure of data as well as result in denial of service.

Mitel states that a security access control vulnerability in these services may allow a remote unauthenticated attacker to gain access to sensitive information and services, potential code execution in the context of the conference component, as well as denial of service of the affected system. In the case of a denial of service attack, a series of malformed messages are handled improperly causing the services to create significant outbound traffic.

RECOMMENDATIONS:
The following actions should be taken:

- Install the updates and/or mitigations mentioned by Mitel immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Apply the Principle of Least Privilege to all systems and services.

REFERENCES:

Mitel:

https://learn.cisecurity.org/e/799323/duct-security-advisory-22-0001/qvh3c/266970440?h=0A9s21D0sqX1k--3mYepKjLNU3J_v0JZWujviHPOFF0

https://learn.cisecurity.org/e/799323/etin-22-0001-02-v1---mivbx-pdf/qvh3f/266970440?h=0A9s21D0sqX1k--3mYepKjLNU3J_v0JZWujviHPOFF0

https://learn.cisecurity.org/e/799323/n-22-0001-01-v1---micollab-pdf/qvh3h/266970440?h=0A9s21D0sqX1k--3mYepKjLNU3J_v0JZWujviHPOFF0