Product Notice #0511

Vulnerabilities Discovered and Subsequent Mitigations in One Voice Operations Center (OVOC) Server

This Product Notice announces possible security vulnerabilities that were recently (privately) discovered and reported to AudioCodes regarding the OVOC server. These vulnerabilities and subsequent mitigations are described in detail below.

Effective Date

Immediate

Vulnerability

1. Exposure of backup files in the */nbif/* directory. Some of the files contain sensitive information, including encrypted usernames and passwords. Access to the directory is username (*nbif*) / password protected.
2. Hardcoded cryptographic keys employed by OVOC for all OVOC installations. Once an attacker obtains these keys, they can be used to decrypt all encrypted secrets (in all OVOC installations).
3. Directory traversal vulnerability in OVOC's Device Manager module can be exploited by an attacker to gain access to the underlying host's operating system files.
4. Insecure file upload through OVOC's Device Manager module can be exploited by an attacker to achieve remote code execution (RCE).

Mitigation

1. This finding can be mitigated by changing the default password of the *nbif* user.
2. This finding can be mitigated by changing the default encryption key per OVOC installation.
3. This finding has been fixed in OVOC Version 8.2.1000. This software is available for download from AudioCodes Services Portal (registered customers only).
4. This finding has been fixed in OVOC Version 8.2.1000. This software is available for download from AudioCodes Services Portal (registered customers only).

Affected Products

One Voice Operations Center (OVOC)

Announcement Date

August 20, 2023

If you have any questions, at https://www.audiocodes.com/corporate/offices-worldwide

AudioCodes Ltd. | 1 Hayarden Street | Airport City | Lod | Israel | +972-3-976-4000