# Unauthenticated SubSonic backend access in Ampache

High lachlan-00 published GHSA-p9pm-j95j-5mjf on Apr 12, 2021

Package

SubSonic Backend

| Affected versions | Patched versions |
|---|---|
| <4.4.1, develop <3c12ef26c | 4.4.1, develop 3c12ef26c |

Description

## Impact

Allows unauthenticated access to Ampache using the subsonic API.

To successfully make the attack you must also use a username that is not part of the site to successfully bypass the auth checks.

## Patches

Develop branch and 4.4.1 are patched

## Workarounds

Disable Subsonic Backend

Replace the token check function in lib/class/auth.class.php

```
    public static function token_check($username, $token, $salt)
    {
        // subsonic token auth with apikey
        if (strlen((string) $token) && strlen((string) $salt) && strlen((string) $username)) {
            $sql        = 'SELECT `apikey`, `username` FROM `user` WHERE `username` = ?';
            $db_results = Dba::read($sql, array($username));
            $row        = Dba::fetch_assoc($db_results);
            $hash_token = hash('md5', ($row['apikey'] . $salt));
            if ($token == $hash_token && $row['username'] == $username && isset($row['apikey'])) {
                return array(
                    'success' => true,
                    'type' => 'api',
                    'username' => $username
                );
            }
        }

        return array();
    }
```

For more information

If you have any questions or comments about this advisory:

Open an issue in the Ampache repo
Email lachlan

## Example attack url

```
http://ampache.org/rest/getplaylists.view?u=notauseraccount&c=Sublime+Music&f=json&v=1.8.0&s=855f145addd8e5&t=cc1f9525d1fb7d4a8ab2576c544b25ee
```

Severity

High

CVE ID

CVE-2021-21399

Weaknesses

No CWEs

Credits

Creling