Unauthenticated SQL injection in Ampache

High lachlan-00 published GHSA-phr3-mpx5-7826 on Sep 16, 2020

Package

database_object.abstract.php

Affected versions

master <4.2.2, develop <e92cb6154

Patched versions

4.2.2, develop e92cb6154

Description

Impact

Vulnerability allows unauthenticated users to perform SQL injection

Patches

Develop branch and 4.2.2 are patched

Workarounds

Replace the get_info function in lib/class/database_object.abstract.php

```
/**
 * get_info
 * retrieves the info from the database and puts it in the cache
 * @param integer $object_id
 * @param string $table_name
 * @return array
 */
public function get_info($object_id, $table_name = '')
{
    $table     = $table_name ? Dba::escape($table_name) : Dba::escape(strtolower(get_class($this)));
    $object_id = (int) $object_id;

    // Make sure we've got a real id
    if ($object_id < 1) {
        return array();
    }

    if (self::is_cached($table, $object_id)) {
        return self::get_from_cache($table, $object_id);
    }

    $params     = array($object_id);
    $sql        = "SELECT * FROM `$table` WHERE `id`= ?";
    $db_results = Dba::read($sql, $params);

    if (!$db_results) {
        return array();
    }

    $row = Dba::fetch_assoc($db_results);

    self::add_to_cache($table, $object_id, $row);

    return $row;
} // get_info
```

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

```
wget "https://ampacheserver/server/ajax.server.php?page=index&action=artist_info&artist=1'; INSERT INTO user (username,access) VALUES ('foolbar','100');'"
```

Severity

High

CVE ID

CVE-2020-15153

Weaknesses

No CWEs

Credits