> Ghosts in the shell

.entry

Search

.entry
.articles
  .CVE-2025-63421
  .CVE-2025-61258
  .CVE-2023-27168
  .CVE-2023-27169
  .CVE-2023-27170
  .CVE-2023-27172
  .dllMemoryScanner
  .MessageBoxInjection
  .RtwqExecution
  .GuiCallbackHijack
  .avEvasion

.CVE-2023-27169
Vulnerability Overview
Context
What is Write-Back?
Technical description
Impact
Mitigation
Timeline
Credits

.CVE-2023-27169

Vulnerability Overview

Use of hardcoded cryptographic key.

Context

The discovered vulnerability allows an attacker to retrieve the secret salt used to encrypt and decrypt the license hashes commercially emitted to clients or customers.

What is Write-Back?

Refer to Write-Back Description

Technical description

The second vulnerability, which has been assigned with CVE-2023-27169 can be categorized as **usage of hard-coded cryptographic key**. The implementation of the license validator on the Manager component, relies on the utilization of a symmetric encryption algorithm with a static salt or secret.

By analysing the files of a local windows installation, we managed to retrieve the salt being used in the license creation and validation routine.

WriteBackLicenseConfig.class

```
package com.xpandit.license.writeback.config;

import com.xpandit.license.api.config.LicenseConfig;

public class WriteBackLicenseConfig implements LicenseConfig {
13  private String salt = "xpandit_write321back1231";

18  private String pluginId = "com.xpandit.plugins.writeback";

    public String getSalt() {
26    return this.salt;
    }

    public String getPluginId() {
33    return this.pluginId;
    }
}
```

Impact

If the license creation and validation routines, relie, solely on the LicenseConfig salt as an encryption key to provide secrecy and integrity to a license hash/key, then it could be possible for an attacker to reverse the encryption process to retrieve any information possibly encrypted in the license string and craft its own commercial write-back licenses.

CVE ID: CVE-2023-27169
CVSS 3.1 Base Score: 5.1
CVSS Vector: AV:L/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N
Affected Vendor: Xpand IT
Affected Product: Write-Back
Affected Version: Write-back Manager v2.3.1

Mitigation

All affected costumers should update Write-Back to at least version 4.1.

Timeline

29-11-2022 - Vulnerability detected and reported to Write-Back.
22-02-2023 - Vulnerability submitted to Mittre.
10-03-2023 - Vulnerability accepted and CVE ID reserved.
12-07-2023 - Official Patch released by Write-Back team.

Credits

me

Site built with MkDocs and Terminal for MkDocs.