


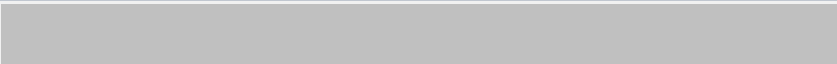

CVE-2022-34002 Personnel Data Systems (PDS) Vista 7 - Local File Inclusion




Created by Nick Berrie
Jul 08, 2022 • 2 min read

Summary

Name	Personnel Data Systems (PDS) Vista 7 - Local File In
Product	PDS Vista 7
Affected Versions	<7.1.7.2 – External Applicants Security Hotfix – XA C
State	Public
Release Date	2022/08/08

Vulnerability

Type	Local File Inclusion
Rule	CWE-22 - Improper Limitation of a Pathname to a F  CWE - CWE-22: Improper Limitation of a Pathna ectory ('Path Traversal') (4.9)
Remote?	Yes
Authentication Required?	Yes
CVSS v3 Vector	AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N
CVSS v3 Base Score	7.7

CVSS v3 Base Score	/./
Exploit Available?	No, but manually exploitable
CVE ID(s)	<div>CVE -</div> <div>CVE-2022-34002</div>

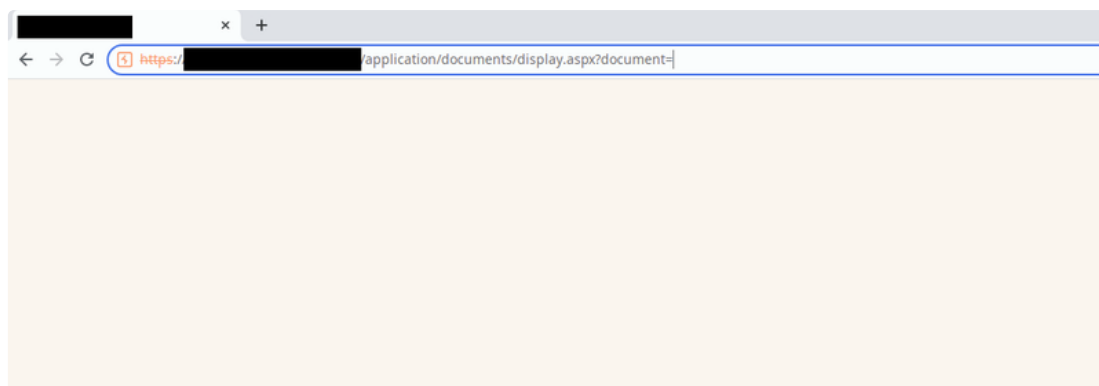
Description

The 'document' parameter of PDS Vista 7's `/application/documents/display.aspx` page is vulnerable to a Local File Inclusion vulnerability which allows an low-privileged authenticated attacker to leak the configuration files and source code of the web application.

Proof-of-Concept

The implementation of PDS Vista 7 may vary by organization so the following proof-of-concept may not follow the same flow as other client implementations. The situation in which Assura discovered this vulnerability, the client had implemented PDS Vista 7 to accept applications for job positions. This required the creation of an account by a job application which exposed the vulnerable function.

1. Proxy a browser in Burp Suite or another web browser proxying tool.
2. Log into the system that implements PDS Vista 7 prior to the application of the patch '7.1.7.2 – External Applicants Security Hotfix – XA Clients Only'.
3. Navigate to the `/application/documents/display.aspx?document=` page.
 - a. At this point, the page should return a 200 OK code but the page itself will be blank in the web browser.



4. Add the value '/web.config' to the document parameter and request the page again. See that this time we receive a response with encrypted content. This is where the vulnerability gets interesting.



5. In Burp Suite, find the request/response pair for the `/application/documents/display.aspx?document=/web.config` request.
 - a. In the response body, search for the string 'padDiv'. Within the 'padDiv' section of the response body, we can see the unencrypted contents of the file requested.



6. This vulnerability can be used to retrieve any file contents within the root or sub-directories of the web application but not system level or above-root level files.

Exploit

There is no pre-packaged exploit for this vulnerability at this time although it can be easily exploited manually as shown in the Proof-of-Concept section above.

Mitigation

Customers should apply the following patch - '7.1.7.2 – External Applicants Security Hotfix – XA Clients Only'

Credits

This vulnerability was discovered by Nick Berrie (<https://www.linkedin.com/in/nick-berrie/>), Technical Director of Assura's Offensive Security Operations department at Assura, Inc.

References

Vendor Page	Vista Overview PDS
CVE Description	CVE - CVE-2022-34002

Timeline

- 2022-04-27: Vulnerability discovered
- 2022-04-27: Vendor contacted
- 2022-06-19: CVE #s issued by MITRE
- 2022-04-29: Vendor confirmed patch
- 2022-08-08: Public disclosure

Related Vulnerabilities


[CVE-2021-43969 Quicklert for Digium Switchvox Version 10 Build 1043 – Blind SQL Injection with Out-of-Band Interaction \(DNS\) \(Vulnerability Research\)](#)

[sqli](#) [quicklert](#) [vuln](#)


[CVE-2021-43970 Quicklert for Digium Switchvox Version 10 Build 1043 – Arbitrary File Upload Results in Remote Code Execution \(Vulnerability Research\)](#)

[rfi](#) [vuln](#) [quicklert](#)

[m](#) [vuln](#) [quickier](#)

 CVE-2022-26959 Northstar Club Management software version 6.3 - Full, Blind/Time-based SQL Injection (Vulnerability Research)

[vuln](#) [northstar](#) [sqli](#)

 CVE-2022-34002 Personnel Data Systems (PDS) Vista 7 - Local File Inclusion (Vulnerability Research)

[vuln](#) [pds](#) [vista](#)

[vuln](#) [pds](#) [vista](#)

