



Vulnerability Announcement

PeopleSoft PeopleTools Search Information Disclosure Vulnerability

Overview

The I-Assure Vulnerability Research Team (VRT) has discovered several, previously unpublished vulnerabilities in the PeopleSoft (Oracle) PeopleTools application. PeopleTools provides you the power and flexibility to enhance, deploy, and extend your PeopleSoft and non- PeopleSoft applications.

```
Bugtraq ID: 8788
Class: Access Validation Error
CVE: CVE-MAP-NOMATCH
Remote: Yes
Local: No
```

Our proactive VRT can assess your application for vulnerabilities before you fall victim to information disclosure or hacking activities. We utilize our experience and knowledge of system/application security to perform our assessment. We do NOT solely rely on automated tools to perform our assessment.

Description

PeopleTools 8.42 has a "grid" option, which allows a user to save a search to an .xls file. The .xls file is displayed in the local browser, allowing a user to do a "Save As" to save to local hard drive. The out- put file is also saved as a temporarily-resident copy on the web server without restrictions.

Any user, without authenticating, can browse to the direct URL location and access the file. The file appears to stay in this location for approximately 5 minutes before you get the '404 File not found' error.

The application makes the file available by storing it on the webserver for a period of time that is hard coded into the java servlet. The file is stored in a directory with a random name, however, the random directory name could be determined using automated tools and since the file itself is not secured, it is potentially accessible by unauthorized users.

Vendor Solution

Available for download from www.peoplesoft.com is a script to make the download to Excel buttons invisible. The script is for Microsoft SQL Server, if you are on a different Database platform, you will have to make the necessary changes to the script.

NOTE: The script is NOT designed to make it easy for you to return to your prior state after the script has been applied. Additionally, this script is provided as a convenience, and is not supported by GSC.

PLEASE REMEMBER, this is considered to be a customization beyond the scope of the Global Support Center. We are delivering a script that works in Microsoft SQL Server with no plans to create different scripts for the different Database platforms.