



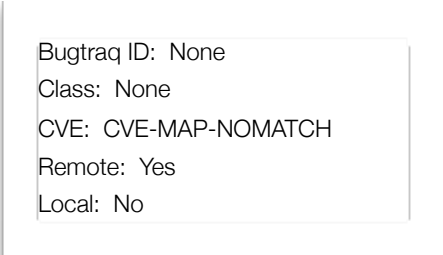
Vulnerability Announcement

PeopleSoft PeopleTools 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The I-Assure Vulnerability Research Team (VRT) has discovered several, previously unpublished vulnerabilities in the PeopleSoft (Oracle) PeopleTools application.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.

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.



```
Bugtraq ID: None
Class: None
CVE: CVE-MAP-NOMATCH
Remote: Yes
Local: No
```

Description

<Control><J> is a hot key that is used by everyone that helps in troubleshooting many issues within the PIA or Portal environment. Ever since PeopleTools 8.1x, <Control><J> allows us to see information like: Browser and its version, name of Operating System, PeopleTools version, Application type and its version, Service Pack number, current Menu name, and current Component name, current Page name, the UserID who is logging in, the name of the Database logged into, the Database platform, and the IP of the Application Server.

Although most of the information may seem to be harmless, some of the information is considered too sensitive and should not be shared with all of the user community. The following information should be hidden from the users: the UserID who is logging in, the name of the Database logged into, the Database platform, and the IP of the Application Server.

Vendor Solution

Control - J functionality is modified by changing the following line in configuration.properties:

```
# If set to true, the database name and other potentially sensitive connection
information
# will appear in the HTML generated for use in a help display.
# Default: true
connectionInformation=true
```

Setting this value to false will hide security related information from CTRL-J and HTML object PT_INFOPAGE will be displayed:

```
Browser IE/6.0
Operating System WINNT
Browser Compression ON (gzip)
Tools Release 8.42.01
Application Release HRMS 8.80.00.000
Service Pack 0
```

I-Assure, LLC

Page NID_LOOKUP
Component NID_LOOKUP
Menu ADMINISTER_WORKFORCE_(GBL)

If connectionInformation=true, the following HTML object PT_INFOPAGECONNECT is displayed:

Browser IE/6.0
Operating System WINNT
Browser Compression ON (gzip)
Tools Release 8.42.01
Application Release HRMS 8.80.00.000
Service Pack 0
Page NID_LOOKUP
Component NID_LOOKUP
Menu ADMINISTER_WORKFORCE_(GBL)
User ID PS
Database Name HRMS
Database Type MICROSOFT
Application Server //127.0.0.1:9000

Further, the actual HTML objects can be modified to restrict display of sensitive objects. Please note that this is a customization to a delivered PeopleTools object and will require special attention when applying PeopleTools patches and upgrades.