

## PeopleTools Critical Patch Update Pre-installation Note

<b>Security Vulnerability ID:</b>	20061017PSE	<b>Date:</b>	October 17, 2006
<b>Name:</b>	PeopleSoft Enterprise Tools, PeopleSoft Enterprise Portal October Critical Patch Update Pre-installation note	<b>Severity:</b>	See Risk Matrix
<b>Intended Audience:</b>	All systems managers or administrators for PeopleSoft Enterprise Tools and PeopleSoft Enterprise Portal implementations		
<b>Affected Products:</b>	PeopleSoft Enterprise Tools 8.22, 8.46, 8.47, 8.48 PeopleSoft Enterprise Portal 8.8, 8.9		
<b>Affected Platforms:</b>	All operating system, web server and database systems.		

### Oracle PeopleSoft Enterprise Tools Risk Matrix

Vuln#	Component	Protocol	Package and/or Privilege Required	Remote and Unauthenticated?	CVSS RISK							Earliest Supported Release Affected	Last Affected Patch set
					Base Score	Access Vector	Attack Complexity	Authentication	Confidentiality	Integrity	Availability		
PSE01	PeopleTools	Network	Valid Session	No	6.0	Remote	Low	Required	Complete	Complete	Complete	8.46GA 8.47GA 8.48GA	8.46.15 8.47.09 8.48.03
PSE02	PeopleTools	Network	None	Yes	4.7	Remote	Low	Not Required	Partial	Partial+	None	8.46GA 8.47GA 8.48GA	8.46.15 8.47.09 8.48.03
PSE04	PeopleTools	Network (http(s))	Valid Session	No	2.8	Remote	Low	Required	Partial	Partial	None	8.46 GA 8.47 GA 8.48 GA	8.46.15 8.47.09 8.48.03
PSE03	PeopleTools	Network	Valid Session	No	3.4	Remote	Low	Required	Complete	None	Partial	8.22GA 8.46GA 8.47GA 8.48GA	8.22.11 8.46.15 8.47.09 8.48.03

PSE05	PeopleSoft Enterprise Portal	Network	Valid Session	No	2.8	Remote	Low	Required	Partial	Partial	None	8.80 GA 8.90 GA	8.8 Bundle 11 8.9 Bundle 4
PSE06	PeopleTools	Network	Valid Session	No	1.4	Remote	Low	Required	Partial+	None	None	8.22GA 8.46GA 8.47GA 8.48GA	8.22.11 8.46.15 8.47.09 8.48.03
PSE07	PeopleTools	Network	Valid Session	No	1.1	Remote	High	Required	Partial+	None	None	8.22GA 8.46GA 8.47GA 8.48GA	8.22.11 8.46.15 8.47.09 8.48.03
PSE08	PeopleTools	Network (http(s))	Valid Session	No	1.1	Remote	High	Required	Partial+	None	None	8.22GA 8.46GA 8.47GA 8.48GA	8.22.11 8.46.15 8.47.09 8.48.03

### **Products affected**

These vulnerabilities affect PeopleSoft Enterprise Tools and PeopleSoft Enterprise Portal.

### **Platforms affected**

PSE01, PSE02, PSE03, PSE04, PSE05, PSE06, PSE07, PSE08: These problems are independent of the web server, operating system and database system in use.

### **Resolution(s)**

PSE01: Apply patch 8.46.16, 8.47.10, 8.48.04

PSE02: Apply patch 8.46.16, 8.47.10, 8.48.04

PSE04: Apply patch 8.46.16, 8.47.10, 8.48.04

PSE03: Apply patch 8.22.12, 8.46.16, 8.47.10, 8.48.04

PSE05:

Solution 682729 for Enterprise Portal 8.8 Prerequisite Bundle 11

Solution 682727 for Enterprise Portal 8.9 Prerequisite Bundle 4

PSE06: Apply patch 8.22.12, 8.46.16, 8.47.10, 8.48.04

PSE07: Apply patch 8.22.12, 8.46.16, 8.47.10, 8.48.04

PSE08: Apply patch 8.22.12, 8.46.16, 8.47.10, 8.48.04

Please refer to GSC resolution 201025553 to address queries which may break due to the uptake of this patch.

In addition, it is recommended that customers review their internal security procedures and ensure that only appropriate employees have administrator access to PeopleSoft Enterprise applications. In particular, ensure that your machines and environments for your Process Schedulers and databases are not directly accessible from users' environments.

Please call your local [Global Support Center](#) for more information.

### **Acknowledgements**

Externally Reported

### **Revision information** FINAL <sup>1</sup>

---

<sup>1</sup> PeopleTools October 2006 Critical Patch Update Pre-Installation Note.doc