

**Critical Patch Update April 2022 Patch Availability Document for Oracle Primavera Products (Doc ID 2856639.1)**

**DETAILS**

**Critical Patch Update January 2022 Patch Availability Document for Oracle Primavera Products**

**1 What's New in This Critical Patch Update**

This Critical Patch Update includes patches for the following Oracle Primavera product versions:

- Primavera Unifier (17.7 – 17.12, 18.8, 19.12, 20.12, 21.12)
- Instantis EnterpriseTrack (17.1, 17.2, 17.3)

**2 Critical Patch Update Availability for Oracle Primavera Releases**

The tables in this section list the patches needed for Oracle Primavera products to address security vulnerabilities and information on downloading and applying the patches. For additional information on the vulnerabilities that are addressed by the patches, click the appropriate link in the Advisory Number column of the table.

**2.1 Primavera Unifier**

**Table 1: Critical Patch Update Availability for Primavera Unifier 17.7 – 17.12, 18.8, 19.12, 20.12, 21.12**

Advisory Number	Primavera Unifier Product Version				
	17.7-17.12	18.8	19.12	20.12	21.12
<a href="#">CVE-2021-23450</a>	Upgrade to 17.12.11.11	Upgrade to 18.8.18.10	Upgrade to 19.12.16.3	Upgrade to 20.12.14	Upgrade to 21.12.4
<a href="#">CVE-2021-41184</a>	<a href="#">Patch 34063509</a>	<a href="#">Patch 34063500</a>	<a href="#">Patch 34063489</a>	<a href="#">Patch 34063482</a>	<a href="#">Patch 34063307</a>

**2.2 Instantis EnterpriseTrack**

**Table 2: Critical Patch Update Availability for Instantis EnterpriseTrack 17.1, 17.2, 17.3**

Advisory Number	Instantis EnterpriseTrack Platform/Middletier Version
	17.1, 17.2, 17.3
<a href="#">CVE-2021-44832</a>	Upgrade to 17.3.4.20  <a href="#">Patch 33980594</a>

### 3 Oracle Construction and Engineering Risk Matrix

This Critical Patch Update contains 3 new security patches for Oracle Construction and Engineering. 1 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 RISK (see <a href="#">Risk Matrix Definitions</a> )									Supported Versions Affected	Notes
					Base Score	Attack Vector	Attack Complex	Privs Req'd	User Interact	Scope	Confidentiality	Integrity	Availability		
CVE-2021-23450	Primavera Unifier	Platform (dojo)	HTTP	No	7.6	Network	Low	Low	None	Un-changed	Low	Low	High	17.7-17.12, 18.8, 19.12, 20.12, 21.12	
CVE-2021-44832	Instantis EnterpriseTrack	Logging (Apache Log4j)	HTTP	No	6.6	Network	High	High	None	Un-changed	High	High	High	17.1, 17.2, 17.3	
CVE-2021-41184	Primavera Unifier	User Interface (jQueryUI)	HTTP	Yes	6.1	Network	Low	None	Required	Changed	Low	Low	None	17.7-17.12, 18.8, 19.12, 20.12, 21.12	