Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Oracle Addresses Agile PLM Flaw Exploited in the Wild

Date of Publication	Admiralty Code	TA Number
November 21, 2024	A1	TA2024440

Summary

First Seen: November 2024
Affected Products: Oracle Agile Product Lifecycle Management (PLM) Framework
Impact: Oracle has issued an alert regarding a high-severity security vulnerability, CVE-2024-21287, impacting the Agile Product Lifecycle Management (PLM) Framework. This unauthenticated file disclosure flaw has been actively exploited in the wild, allowing attackers to download sensitive files without authorization. Organizations leveraging Agile PLM should prioritize applying the latest security updates to mitigate the risk of exploitation and secure their systems.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2024-21287	Oracle Agile PLM Framework File Disclosure Vulnerability	Oracle Agile Product Lifecycle Management (PLM) Framework	✗	✗	✓

Vulnerability Details

#1 Oracle has issued a patch for CVE-2024-21287, a high-severity vulnerability in its Agile Product Lifecycle Management (PLM) framework. This flaw is exploited in wild and enables attackers to remotely disclose sensitive files without requiring authentication. Oracle Agile PLM is a cornerstone tool for driving product innovation in numerous industries, underscoring the importance of addressing this threat promptly to prevent unauthorized access to critical business data.

#2 CVE-2024-21287 is particularly dangerous because it allows attackers to exploit the vulnerability over a network without needing credentials. Successful exploitation could result in unauthorized access to sensitive files, exposing confidential data and intellectual property. The lack of an authentication requirement amplifies the risk, as malicious actors can target systems with minimal effort.

#3 Organizations leveraging Agile PLM are strongly urged to apply Oracle's security updates immediately to mitigate this threat. Beyond patching, implementing robust network monitoring and access controls can help detect and prevent potential exploitation. Proactive measures are crucial to safeguarding sensitive data and maintaining the integrity of critical business systems.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-21287	Oracle Agile PLM Framework Version 9.3.6	cpe:2.3:a:oracle:agile_plm_framework:*:*:*:*:*:*:*:*	CWE-863

Recommendations

Apply Patches: Users are strongly encouraged to update their Oracle Agile Product Lifecycle Management (PLM) Framework to the latest version that addresses CVE-2024-21287. Prompt patching is crucial to prevent exploitation of this unauthenticated file disclosure vulnerability and to protect sensitive data from unauthorized access.

Review Access Controls: Review and strengthen access controls around sensitive data and the Agile PLM system. Limit access to only authorized personnel and ensure that sensitive files are properly secured.

Monitor Network Traffic: Deploy advanced network monitoring tools to detect any unusual or unauthorized activities, particularly those that involve attempts to exploit CVE-2024-21287. Focus on traffic patterns that may indicate unauthorized file access or exploitation attempts and set up alerts for any suspicious activity involving Agile PLM systems.

Vulnerability Management: Implement a robust vulnerability management process to ensure that software and systems are regularly assessed for vulnerabilities and updated with the required security patches. Prioritize critical vulnerabilities identified by security advisories and vendors to mitigate the risk of exploitation by threat actors.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	**TA0004** Privilege Escalation	**TA0040** Impact	**T1588** Obtain Capabilities
T1588.006 Vulnerabilities	**T1565** Data Manipulation	**T1068** Exploitation for Privilege Escalation	

Patch Link

https://support.oracle.com/rs?type=doc&id=3058429.1

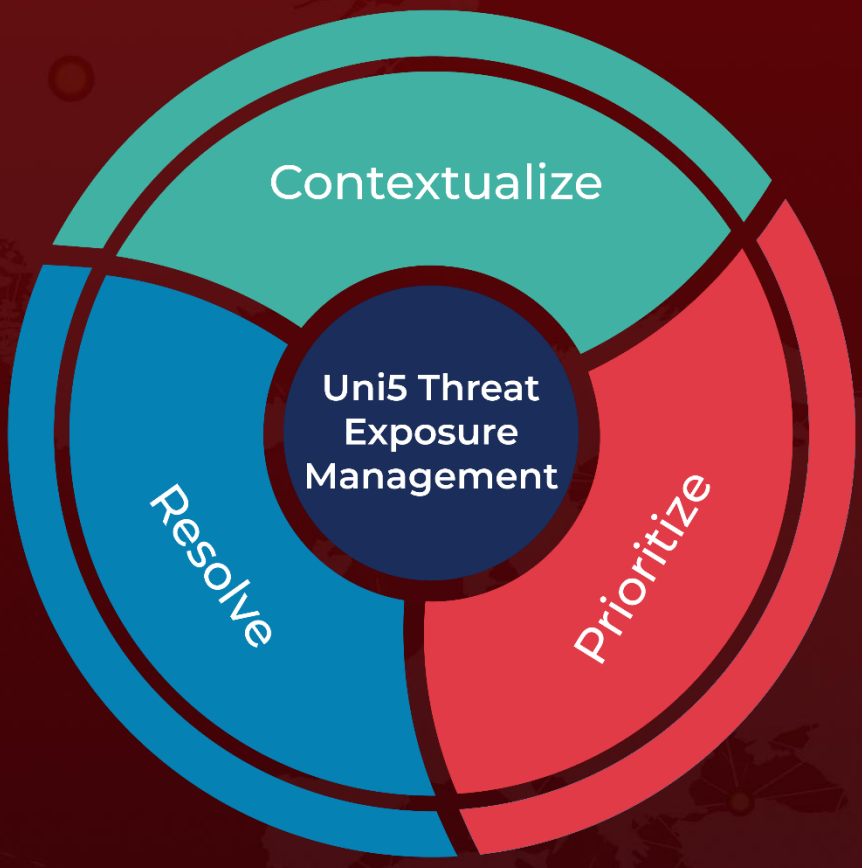
References

https://www.oracle.com/security-alerts/alert-cve-2024-21287.html

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

November 21, 2024 . 7:15 AM

More at www.hivepro.com