



CVE-2022-21587: Rapid7 Observed Exploitation of Oracle E-Business Suite Vulnerability

Feb 07, 2023 | 2 min read | [Glenn Thorpe](#)   


Last updated at Tue, 03 Sep 2024 19:35:40 GMT

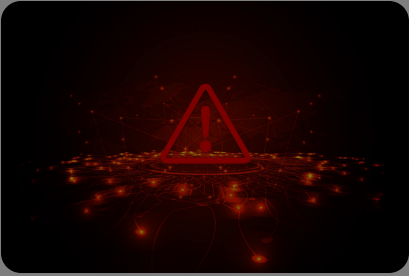
Emergent threats evolve quickly, and as we learn more about this vulnerability, this blog post will evolve, too.

Rapid7 is responding to various compromises arising from the exploitation of [CVE-2022-21587](#) , a critical arbitrary file upload vulnerability (rated 9.8 on the CVSS v3 risk metric) impacting Oracle E-Business Suite (EBS). Oracle published a [Critical Patch Update Advisory](#)  in October 2022 which included a fix, meanwhile, CISA added CVE-2022-21587 to its Known Exploited Vulnerabilities (KEV) catalog on February 2, 2023.

Oracle E-Business Suite is a packaged collection of enterprise applications for a wide variety of tasks such as customer relationship management (CRM), enterprise resource planning (ERP), and human capital management (HCM).

CVE-2022-21587 can lead to unauthenticated remote code execution.

On January 16, 2023, [Viettel Security published an analysis](#)  of the issue detailing both the vulnerability's root cause and a method of leveraging the vulnerability to gain code execution. An exploit based on the Viettel



Topics

- Metasploit (654)
- Vulnerability Management (359)
- Research (236)
- Detection and Response (205)
- Vulnerability Disclosure (148)
- Emergent Threat Response (141)
- Cloud Security (136)
- Security Operations (20)

Popular Tags

- Search Tags
- Metasploit
- Metasploit Weekly Wrapup
- Vulnerability Management
- Research
- Logentries
- Detection and Response

Rapid7 uses cookies and similar technologies as strictly necessary to make our site work. We and our partners would also like to set additional cookies to analyze your use of our site, to personalize and enhance your visit to our site and to show you more relevant content and advertising. These will be set only if you accept.

You can always review and change your cookie preferences through our cookie settings page. For more information, please read our [Privacy Statement](#)

Accept Cookies

Decline Cookies

Cookie Settings



PLATFORM

PRODUCTS

SERVICES

RESOURCES

COMPANY

PARTNERS

EN

SIGN IN

Blog

Vulnerability Management

MDR

Detection & Response

Cloud Security

App Security

Metasploit

All Topics

START TRIAL

Perl web shell that has been observed so far.

Affected products

Oracle Web Applications Desktop Integrator as shipped with Oracle E-Business Suite versions 12.2.3 through 12.2.11 are vulnerable.

What we’re seeing

The attacker(s) are using the above-mentioned proof of concept exploit, uploading a perl script, which fetches (via curl/wget) additional scripts to download a malicious binary payload making the victim host part of a botnet.

Rapid7 customers

InsightVM & Nexpose customers: Authenticated vulnerability checks for CVE-2022-21587 have been available since November 2022. Note that these require valid Oracle Database credentials to be configured in order to collect the relevant patch level information.

InsightIDR & Managed Detection & Response (MDR) customers: in our current investigations, the previously existing detections have been triggering post exploitation:

Suspicious Process - Wget to External IP Address

Attacker Technique - Curl or Wget To Public IP Address With Non Standard Port

We’re also testing new rules more specific to Oracle E-Business Suite.

Updates

February 8, 2023 18:15 UTC

2024-47373

Exploited in Zero-Day Attacks

READ

MORE

Multiple Vulnerabilities in Common Unix Printing System (CUPS)

READ

MORE

High-Risk Vulnerabilities in Common Enterprise Technologies

READ

MORE

CVE-2024-40766: Critical Improper Access Control Vulnerability Affecting SonicWall Devices

READ

MORE

Rapid7 uses cookies and similar technologies as strictly necessary to make our site work. We and our partners would also like to set additional cookies to analyze your use of our site, to personalize and enhance your visit to our site and to show you more relevant content and advertising. These will be set only if you accept.

You can always review and change your cookie preferences through our cookie settings page. For more information, please read our [Privacy Statement](#)

Page 2 of 4

POST TAGS

Emergent Threat Response

AUTHOR

Glenn Thorpe

SHARING IS CARING



[VIEW GLENN'S POSTS](#)

Related Posts

EMERGENT THREA...

Fortinet FortiManager CVE-2024-47575 Exploited in Zero-Day

READ FULL
POST

EMERGENT THREA...

Multiple Vulnerabilities in Common Unix Printing System

READ FULL
POST

EMERGENT THREA...

High-Risk Vulnerabilities in Common Enterprise

READ FULL
POST

EMERGENT THREA...

CVE-2024-40766:
Critical Improper
Access Control

READ FULL
POST

[VIEW ALL POSTS](#)

