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.

Topics

Popular Tags

, 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).

Metasploit

Metasploit Weekly Wrapup

Vulnerability Management

Research **Logentries**

Detection and Response

Related Posts

Fortinet FortiManager CVE-2024-47575 Exploited in Zero-Day Attacks READ MORE

Multiple Vulnerabilities in Common Unix Printing System (CUPS) READ MORE

High-Risk Vulnerabilities in

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 Security analysis technique was published on GitHub by “HMs” on February 6, 2023.

On February 8, 2023, Rapid7 posted a technical analysis of CVE-2022-21587 on AttackerKB. Of particular note, we found that it is possible to upload arbitrary Java Server Pages (JSP) allowing for exploitation beyond the Perl web shell that has been observed so far.

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

- 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

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`

Updates

February 8, 2023 18:15 UTC

- Rapid7 has posted a technical analysis of CVE-2022-21587 on AttackerKB . Of particular note, we found that it is possible to upload arbitrary Java Server Pages (JSP) allowing for exploitation beyond the Perl web shell that has been observed so far.

POST TAGS

Emergent Threat Response

SHARING IS CARING

AUTHOR

VIEW GLENN'S POSTS

Related Posts

EMERGENT THREAT RESPONSE

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

READ FULL POST

EMERGENT THREAT RESPONSE

Multiple Vulnerabilities in Common Unix Printing System (CUPS)

READ FULL POST

EMERGENT THREAT RESPONSE

High-Risk Vulnerabilities in Common Enterprise Technologies

EMERGENT THREAT RESPONSE

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

VIEW ALL POSTS

Search all the things

BACK TO TOP

RAPID7

CUSTOMER SUPPORT

+1-866-390-8113 (Toll Free)

SALES SUPPORT

+1-866-772-7437 (Toll Free)

Need to report an Escalation or a Breach?

GET HELP

SOLUTIONS

The Command Platform

Exposure Command

Managed Threat Complete

SUPPORT & RESOURCES

Product Support

Resource Library

Our Customers

Events & Webcasts

Training & Certification

Cybersecurity Fundamentals

Vulnerability & Exploit Database

ABOUT US

Company

Diversity, Equity, and Inclusion

Leadership

News & Press Releases

Public Policy

Open Source

Investors