# HC3: Analyst Note

October 28, 2024 TLP:CLEAR Report: 202410281500

## The Miracle Exploit

### Executive Summary

The "Miracle Exploit" refers to a set of critical vulnerabilities in Oracle products, primarily affecting Oracle Fusion Middleware and its ADF Faces framework, which is used to build web interfaces for Java EE applications. This exploit, disclosed in 2022, includes CVE-2022-21445 and CVE-2022-21497, both of which allow attackers to execute remote code without authentication. This can lead to full system compromise, potentially exposing sensitive data and enabling lateral movement within a network.

The vulnerabilities were dubbed the "Miracle Exploit" due to their severity and widespread impact. Organizations using affected Oracle products were advised to apply patches urgently to avoid exploitation. Given its critical nature, cybercriminals could potentially use these exploits as a part of larger attack chains, which might include deploying ransomware after initial system compromise. Its ability to allow unauthorized access and control of systems makes it a severe vulnerability that attackers could exploit for various malicious activities, including ransomware in the future.

### Report

In October 2021, two security researchers—PeterJson of VNG Corporation and Nguyen Jang of VNPT—discovered the CVE-2022-21445 and CVE-2022-21497 vulnerabilities by accident while they were “building a PoC [proof of concept exploit code] for another mega 0-day”. While working with the Zero Day Initiative (ZDI), PeterJson’s and Jang’s research led to the discovery of CVE-2022–21445, which they labeled a “mega bug” vulnerability due to its ease of exploitation and the potentially severe impact it could have on Oracle ADF Faces architecture, a component of Oracle Fusion Middleware. Due to its extremely dangerous nature, it was issued a CVSS vulnerability score of 9.8. It was found that the deserialization of trusted data issue could be chained with CVE-2022–21497, exploiting a takeover flaw in Oracle Web Services Manager, to achieve pre-authentication RCE. PeterJson and Jang named this attack “The Miracle Exploit,” since all of Oracle’s online systems and cloud services that rely on ADF Faces are impacted. In fact, they indicated that any website that uses the ADF Faces framework was vulnerable.

CVE-2022-21445 is described as a deserialization of untrusted data, which could be exploited to achieve arbitrary code execution. Identified in the Application Development Framework (ADF) Faces component, the issue can be exploited remotely without authentication, allowing for remote code execution (RCE) on affected products without authentication. As a result, an attacker can take control of a system by sending specially crafted HTTP requests.

CVE-2022-21497 can be used to trigger server-side request forgery (SSRF) for lateral movement to other vulnerable Oracle systems. A remote, unauthenticated attacker could use these vulnerabilities to take control of a system. The vulnerability is caused by a deserialization flaw in the ADF Faces component, which handles user interface development for Java EE applications. Attackers can exploit this flaw to send untrusted, malicious data, leading to arbitrary code execution on the affected system. This vulnerability affects a wide range of Oracle applications, including Oracle Business Intelligence, Enterprise Manager, WebCenter Portal, and other services built using ADF Faces. This vulnerability has a CVSS score of 8.1,

CVE-2022–21445 impacts a variety of products and services based on Fusion Middleware, various Oracle systems, and even Oracle’s cloud infrastructure. Unauthenticated attackers with network access, via HTTP, can abuse the vulnerability chain. PeterJson and Jang named these vulnerabilities the Miracle Exploit and

released a technical report in June 2022. The report identified vulnerabilities leveraging ADF Faces, a framework that is used to build user interfaces for Java EE applications and integrate with the Oracle Fusion Middleware stack. According to PeterJson and Jang, the pre-authentication RCE issue which they described as a "mega" vulnerability, impacts all applications that rely on ADF Faces. Any unauthenticated attacker with network access via HTTP can abuse the vulnerability. Any product that uses ADF Faces becomes vulnerable to attack, and the researchers were able to use the Oracle exploit to get at least some access to products in the business intelligence, enterprise manager, identity management, SOA Suite, WebCenter Portal, Application Testing Suite, and transportation management sectors.

Oracle released a Critical Patch Update in April 2022 to address 520 vulnerabilities across multiple products. Among these vulnerabilities were CVE-2022-21445 and CVE-2022-21497, which had been discovered by PeterJson and Jang in October 2021.

## CISA Miracle Exploit Vulnerability Warning

On September 18, 2024, CISA issued a warning to organizations that two Oracle vulnerabilities tracked as CVE-2022-21445 and CVE-2020-14644, also known as the "Miracle Exploit", were being exploited in the wild and were added to its Known Exploited Vulnerabilities (KEV) Catalog. CVE-2020-14644 impacts WebLogic Server. Both security holes have been rated 'critical' and they can be exploited by an unauthenticated attacker with remote code execution to take over the targeted system. While CVE-2022-21445 and CVE-2020-14644 were discovered two years apart, they are connected. Currently, there are no public reports describing attacks involving CVE-2022-21445 and CVE-2020-14644, but CISA does occasionally add vulnerabilities to its KEV catalog based on privately received reports.

## Attacker Exploitation of the Miracle Exploit

At this time, there is no direct evidence or reports publicly linking a specific cybercriminal gang, APT (Advanced Persistent Threat) groups and or cyber campaigns to the use of CVE-2022-21445 in any attacks. However, given its critical nature, cybercriminals could potentially use this exploit as a part of larger attack chains, which might include deploying ransomware after initial system compromise. Its ability to allow unauthorized access and control of systems makes it a severe vulnerability that attackers could exploit for various malicious activities, including ransomware in the future. The exploitation of such vulnerabilities typically serves as a precursor to more severe attacks, including data theft and the potential deployment of malware or ransomware. Ransomware attacks typically exploit vulnerabilities that allow for initial access or privilege escalation, which makes CVE-2022-21445 a potential vector in such scenarios, but there are no known instances of it being directly linked to ransomware campaigns. Major organizations such as Dell, BestBuy, Starbucks, and others have been identified as having been potentially impacted by the Miracle Exploit.

Given that exploit code is confirmed to be available 'in the wild' to attackers via sites such as GitHub, vulnerable instances should be prioritized for remediation.

## Impact on Healthcare Organizations

Healthcare organizations could be vulnerable to the Miracle Exploit, especially if they use Oracle Fusion Middleware products that rely on the ADF Faces framework. The vulnerabilities involved in the exploit, such as CVE-2022-21445, allow remote code execution (RCE) without authentication, making it possible for attackers to gain unauthorized access to affected systems. Since healthcare organizations often depend on complex IT infrastructures and middleware for managing critical operations and sensitive patient data,

they could be at significant risk if the vulnerabilities are not patched. Healthcare organizations rely heavily on enterprise software for managing electronic health records (EHRs), patient billing, and other critical services. If these systems are integrated with vulnerable Oracle middleware components, the consequences of exploitation could include data breaches, operational disruptions, and regulatory penalties, particularly under HIPAA laws.

Healthcare organizations are generally attractive targets for cybercriminals due to the sensitive nature of medical data, so while no confirmed attacks involving the Miracle Exploit have been reported, it is essential for healthcare institutions to ensure they apply all relevant patches and updates to mitigate risks. While no specific healthcare-related incidents involving the Miracle Exploit have been reported, the broad applicability of Oracle's middleware in various sectors, including healthcare, underscores the importance of patching and securing systems to prevent such attacks. Healthcare providers should apply Oracle's April 2022 Critical Patch Update to mitigate the risks posed by these vulnerabilities.

## HC3 Recommendations

- **Patch Management**: Apply the latest security patch for Oracle JDeveloper, which addresses the improper input validation issue.
- **Network Segmentation**: Ensure that development environments using JDeveloper are isolated from production systems.
- **Access Control**: Limit access to JDeveloper environments to trusted users only and enforce strong authentication mechanisms.

## TTPs for the Miracle Exploit

The Tactics, Techniques, and Procedures (TTPs) associated with the exploitation of CVE-2022-21445 in Oracle Fusion Middleware generally follow common patterns seen in attacks exploiting deserialization vulnerabilities for remote code execution (RCE). Below are the TTPs related to this vulnerability:

### Tactics:

- **Initial Access**
  - Attackers use unauthenticated remote access via HTTP requests to exploit the deserialization vulnerability in Oracle's ADF Faces component.
  - This provides an entry point for attackers to deliver serialized malicious data to vulnerable systems.
- **Execution**: The attacker crafts malicious payloads that are deserialized by the vulnerable ADF Faces component, leading to remote code execution (RCE) on the target system without requiring prior authentication.
- **Persistence**: Post-exploitation, the attacker may deploy additional malicious software (such as web shells or backdoors) to maintain long-term access.
- **Privilege Escalation**: Once inside the system, attackers could exploit further vulnerabilities or misconfigurations to escalate privileges, enabling them to gain higher-level access or control over other connected systems.
- **Lateral Movement**: Attackers can pivot within the network, especially in cases where Oracle Fusion Middleware services are linked with other enterprise systems or databases, exploiting the interconnected nature of middleware solutions.

- **Data Exfiltration**: Attackers may extract sensitive data from Oracle applications or connected databases if the middleware interfaces with critical business applications like Oracle Business Intelligence or Enterprise Manager.
- **Impact**: The goal could be system takeover for purposes such as data theft, sabotage, or deploying ransomware.

Techniques:

- **Deserialization of Untrusted Data:** The core technical flaw involves the deserialization of user-supplied data, which allows the attacker to craft input that, when processed by the vulnerable system, leads to code execution.
- **Remote Services Exploitation:** Attackers utilize vulnerable web services, such as Oracle ADF Faces, accessible over the internet or network, allowing remote exploitation.
- **Exploitation of Public-Facing Application:** The ADF Faces component can be targeted directly via public-facing Oracle applications that are exposed to the internet.

Procedures:

- **Crafting Malicious Payload**: Attackers generate specially crafted serialized objects that exploit the deserialization vulnerability in ADF Faces, triggering arbitrary code execution when deserialized by the application.
- **Reconnaissance**: Scanning for internet-exposed Oracle Fusion Middleware instances or components using known vulnerable versions is typically the first step.
- **Post-Exploitation**: Once RCE is achieved, attackers may drop additional tools (e.g., malware or shells) for further network exploitation or reconnaissance.

These TTPs are typical of attacks targeting server-side deserialization vulnerabilities, and in the case of CVE-2022-21445, the vulnerability is particularly dangerous due to its presence in widely used Oracle enterprise software, which often connects to sensitive business applications.

## Analyst Comment

There is no direct MITRE ATT&CK mapping specifically for CVE-2022-21445, but we can associate the Tactics, Techniques, and Procedures (TTPs) used in the exploitation of this vulnerability with relevant MITRE ATT&CK techniques based on the nature of the attack.

Here is how CVE-2022-21445 maps to relevant MITRE ATT&CK techniques:

| Tactic | Technique | Procedure |
|---|---|---|
| Initial Access | T1190 (Exploit Public-Facing Application) | The attacker exploits the deserialization vulnerability in the ADF Faces component, a public-facing part of Oracle Fusion Middleware, through unauthenticated HTTP requests. |

| Tactic | Technique | Procedure |
|---|---|---|
| Execution | T1059 (Command and Scripting Interpreter) | Post-exploitation, the attacker executes commands on the compromised server by exploiting the vulnerability that enables remote code execution (RCE). |
| Execution - Sub-Technique | T1059.006 (Deserialization of Untrusted Data) | The binary contains encrypted strings. |
| Persistence | T1547 (Implant Additional Tools) | Ransomware enumerates folders for file encryption. |
| Privilege Escalation | T1068 (Exploitation for Privilege Escalation) | Once inside the system, the attacker might exploit other vulnerabilities to escalate privileges, allowing further control over the system. |
| Lateral Movement | T1021 (Remote Services) | After initial compromise, the attacker can move laterally by exploiting other systems within the network, particularly Oracle services connected via middleware. |
| Impact | T1491.001 (Data Manipulation) | Attackers may alter or manipulate data after gaining access to sensitive systems. |
| Impact | T1485 (Data Destruction) | Attacker could destroy data or configurations as part of a broader attack. |

These mappings reflect how CVE-2022-21445 could fit into the MITRE ATT&CK framework, based on the tactics and techniques involved in exploiting deserialization vulnerabilities for remote code execution. While there is no specific entry for this CVE, the methods attackers would use align with the techniques listed above.

## IOCs

CVE-2022-21445 is a critical remote code execution vulnerability in Oracle Fusion Middleware, specifically in the ADF Faces component. While there is no comprehensive list of Indicators of Compromise (IOCs) specifically tied to this vulnerability, the typical IOCs for this type of exploitation often involve:

1. **Unusual Network Traffic:**
   - Unauthenticated HTTP requests attempting to exploit the deserialization flaw.
   - Traffic targeting ADF Faces components in Oracle systems.
2. **File Changes or Artifacts:**
   - Insertion of malicious serialized data or payloads in Java-based applications.
   - Unexpected changes to configuration files or scripts in Oracle Fusion Middleware environments.
3. **System Logs:**
   - Error logs indicating failed or successful attempts to deserialize untrusted input.

- Unexpected exceptions or stack traces in logs relating to deserialization issues.

4. **Compromise Indicators:**
   - New processes or binaries running on the system that were not previously observed.
   - Signs of privilege escalation or lateral movement within the network after the initial compromise.
5. **Malicious Payloads:** Shellcode or malware being dropped after successful exploitation.

To better detect and respond to potential exploitation, network administrators should monitor for suspicious activity around Oracle Middleware servers, and ensure logging is enabled for deserialization errors and related web traffic. Additionally, any attempts to access Oracle Fusion Middleware without proper authentication should raise red flags.

For more detailed and specific detection strategies, it is important to leverage threat intelligence services and employ monitoring tools capable of detecting anomalous network or system behavior.

## References

Oracle patches 'miracle exploit' impacting Middleware Fusion, cloud services (June 27, 2022
https://portswigger.net/daily-swig/oracle-patches-miracle-exploit-impacting-middleware-fusion-cloud-services

Miracle - One Vulnerability To Rule Them All (Jun2 23, 2022)
https://peterjson.medium.com/miracle-one-vulnerability-to-rule-them-all-c3aed9edeea2

"Miracle Exploit" Vulnerabilities in Multiple Oracle Products (June 28,2022)
https://digital.nhs.uk/cyber-alerts/2022/cc-4119

Oracle Critical Patch Update Advisory (April 2022)
https://www.oracle.com/security-alerts/cpuapr2022.html

CISA: Oracle Vulnerabilities From 'Miracle Exploit' Targeted in Attacks (September 19, 2024)
https://www.securityweek.com/cisa-oracle-vulnerabilities-from-miracle-exploit-targeted-in-attacks/

CISA Adds Five Known Exploited Vulnerabilities to Catalog (September 18th, 2024)
https://www.cisa.gov/news-events/alerts/2024/09/18/cisa-adds-five-known-exploited-vulnerabilities-catalog

Oracle vuln left scores of blue chips exposed to pre-auth RCE exploit for 6 MONTHS post disclosure (June 23, 2022)
https://www.thestack.technology/oracle-middleware-vulnerability-blue-chips-exposed-6-months/

Oracle Fixes' Miracle Exploit' That Affected Middleware Fusion And Cloud Services (June 27, 2022)
https://cyberintelmag.com/cloud-security/oracle-fixes-miracle-exploit-that-affected-middleware-fusion-and-cloud-services/

CVE-2022-21445
https://www.cve.org/CVERecord?id=CVE-2022-21445

Actively Exploited CVE-2022-21445, Deep Dive (September 25, 2024)
Actively Exploited CVE-2022-21445, Deep Dive | Ostorlab: Mobile App Security Testing for Android and iOS

Known Actively Exploited Vulnerabilities Round-up (13.09.24-19.09.24) (September 20, 2024)
https://appcheck-ng.com/known-actively-exploited-vulnerabilities-round-up-13-09-24-19-09-24/

Oracle ADF CVE-2022–21445 Impact on Oracle Global Trade and Transportation Management (July 20, 2024)
https://support.oracle.com/knowledge/Oracle%20E-Business%20Suite/2880481_1.html

CISA: Oracle JDeveloper & WebLogic Server Remote Code Execution Vulnerabilities (CVE-2022-21445 and CVE-2020-14644) (September 19, 2024)
https://op-c.net/blog/cisa-oracle-jdeveloper-weblogic-server-remote-code-execution-vulnerabilities-cve-2022-21445-and-cve-2020-14644/

## Contact Information

If you have any additional questions, we encourage you to contact us at HC3@hhs.gov.

We want to know how satisfied you are with the resources HC3 provides. Your answers will be anonymous, and we will use the responses to improve all future updates, features, and distributions. Share Your Feedback