Insecure Deserialization Attacks

Often leads to remote code execution

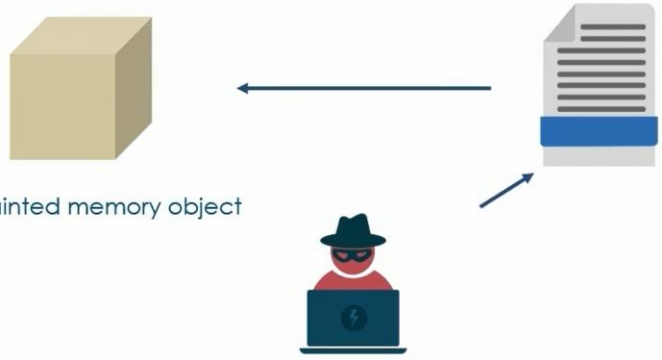
Serialization

- Memory object is written to file (.XML, .JSON) for storage or transmission over a network
- Object methods are removed
- Properties are left intact
- Python: pickle.dump(object,file)

Deserialization

- Memory object is created from a file
- Object properties and methods are available
- Python: pickle.load(file)

Insecure Deserialization

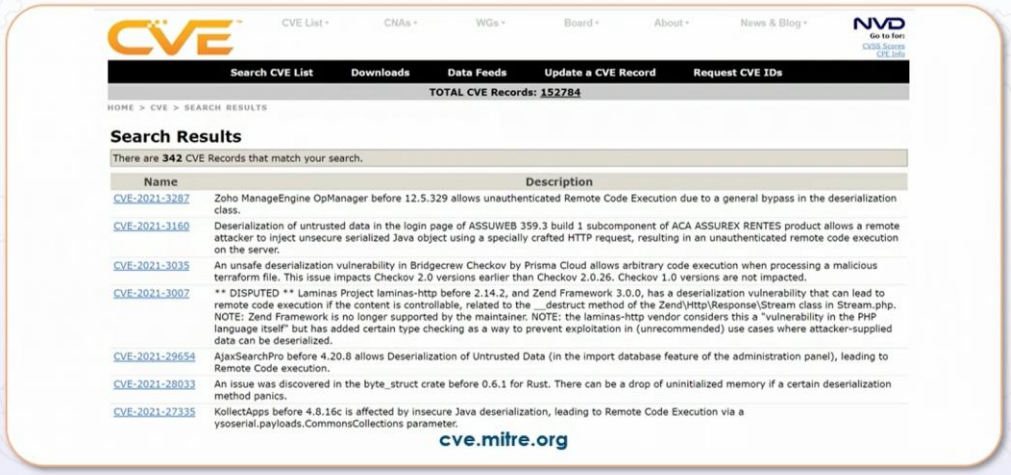


Attacker injects malicious code into byte stream as object is reconstructed

Mitigating Insecure Deserialization Attacks

Never trust user/app input, apply updates

Common Vulnerabilities and Exposures (CVE)



CVE List · CNAs · WGs · Board · About · News & Blog · NVD

Go to for: CVSS Scores CPE Info

Search CVE List | Downloads | Data Feeds | Update a CVE Record | Request CVE IDs

TOTAL CVE Records: 152784

HOME > CVE > SEARCH RESULTS

Search Results

There are **342** CVE Records that match your search.

Name	Description
CVE-2021-3287	Zoho ManageEngine OpManager before 12.5.329 allows unauthenticated Remote Code Execution due to a general bypass in the deserialization class.
CVE-2021-3160	Deserialization of untrusted data in the login page of ASSUWEB 359.3 build 1 subcomponent of ACA ASSUREX RENTES product allows a remote attacker to inject unsecure serialized Java object using a specially crafted HTTP request, resulting in an unauthenticated remote code execution on the server.
CVE-2021-3035	An unsafe deserialization vulnerability in Bridgecrew Checkov by Prisma Cloud allows arbitrary code execution when processing a malicious terraform file. This issue impacts Checkov 2.0 versions earlier than Checkov 2.0.26. Checkov 1.0 versions are not impacted.
CVE-2021-3007	** DISPUTED ** Laminas Project laminas-http before 2.14.2, and Zend Framework 3.0.0, has a deserialization vulnerability that can lead to remote code execution if the content is controllable, related to the __destruct method of the Zend\Http\Response\Stream class in Stream.php. NOTE: Zend Framework is no longer supported by the maintainer. NOTE: the laminas-http vendor considers this a "vulnerability in the PHP language itself" but has added certain type checking as a way to prevent exploitation in (unrecommended) use cases where attacker-supplied data can be deserialized.
CVE-2021-29654	AjaxSearchPro before 4.20.8 allows Deserialization of Untrusted Data (in the import database feature of the administration panel), leading to Remote Code execution.
CVE-2021-28033	An issue was discovered in the byte_struct crate before 0.6.1 for Rust. There can be a drop of uninitialized memory if a certain deserialization method panics.
CVE-2021-27335	KollectApps before 4.8.16c is affected by insecure Java deserialization, leading to Remote Code Execution via a ysoserial.payloads.CommonsCollections parameter.

cve.mitre.org

Disallow Remote Code Execution

Enable executable Allow/Deny lists

Use application containers

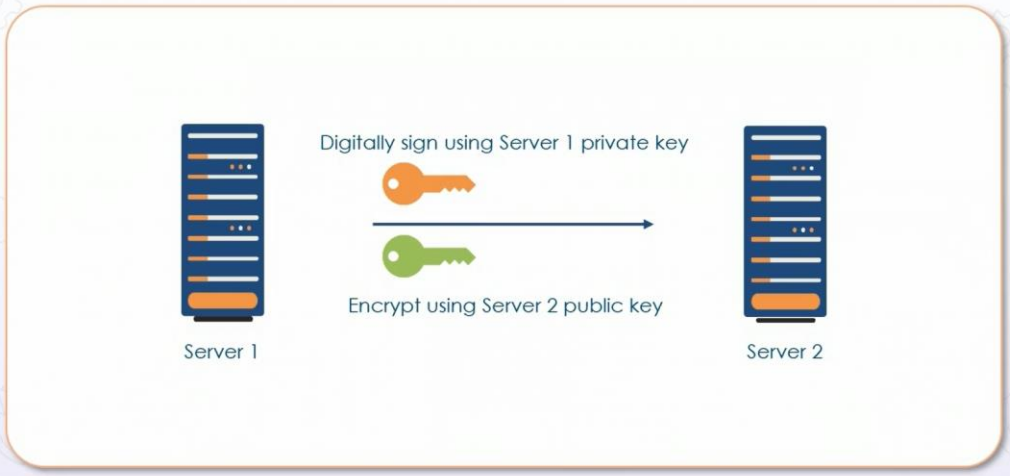
Mitigating Insecure Deserialization Attacks

Mitigating Insecure Deserialization

Deserialize only from hardened trusted sources

Use language-specific secure deserialization functions

Enable Network Digital Signatures




```
#Sample Snort IDS rule to notify of Apache Struts exploit attempt




alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (
msg:"SERVER-APACHE Apache Struts java.lang.ProcessBuilder class
access attempt"; flow:to_server,established; http_uri;
content:"${"; content:"java.lang.ProcessBuilder",nocase;
service:http; reference:cve,2018-11776; classtype:attempted-user;
sid:47690; rev:2; )
```