



A08:2021 – Software and Data Integrity Failures

OWASP Top 10 - Series

**Presenter – Jalaj
@ null-meet, Delhi Chapter :
eSec Forte® Technologies, Gurugram
7 October 2023**

>_ whoami

- Jalaj
- Cyber security geek
- Blue Teamer (SOC Analyst)
- Exploring the world of IR and Threat Hunting
- CRAC Learning
- MMA and Bikes
- Have a question / want to connect ?
 - Telegram : @senditfast



01

Introduction
to
OWASP Top 10

03

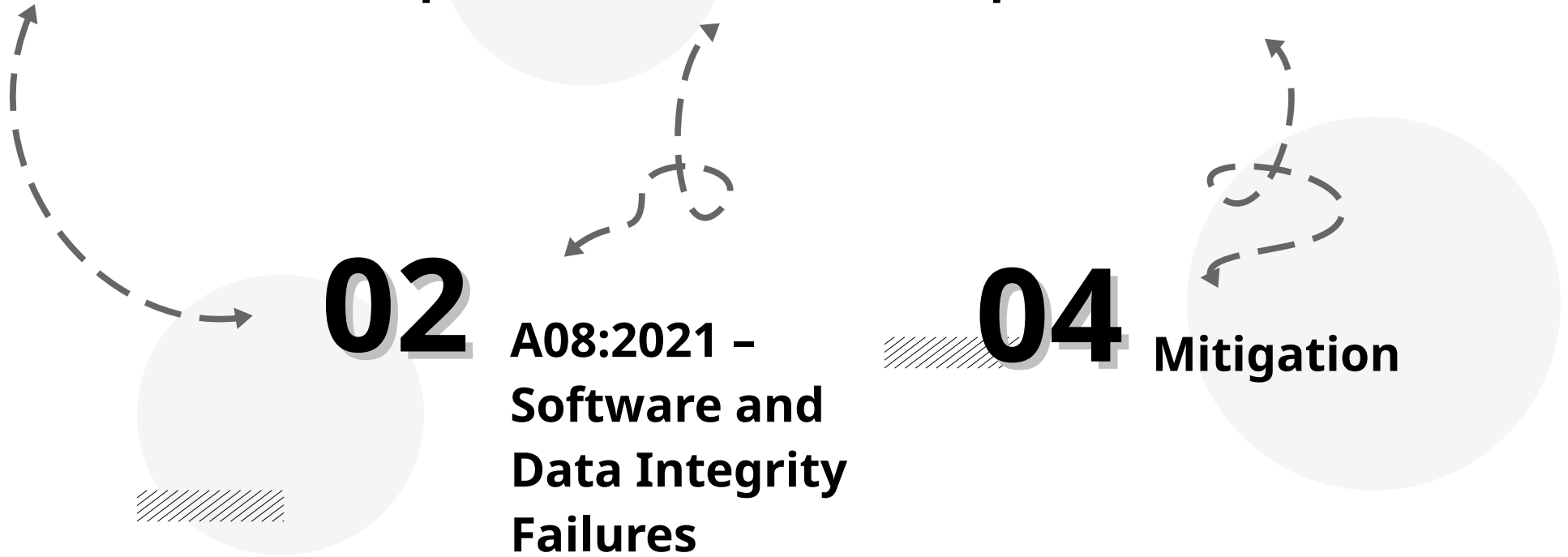
Attacks
With
Examples

02

A08:2021 -
Software and
Data Integrity
Failures

04

Mitigation



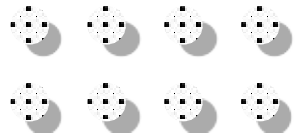
OWASP Top 10

The OWASP Top 10 is a de facto industry standard that provides a list of the 10 Most Critical Web Application Security Risks

- Broken Access Control
- Cryptographic Failure
- Injection
- Insecure Design
- Security Misconfiguration
- Vulnerable and Outdated Components
- Identification and Authentication Failures
- Software and Data Integrity Failures
- Security Logging and Monitoring Failures
- Server-Side Request Forgery (SSRF)



Illustrations by Pixeltrue on [icons8](#)





Software and Data Integrity Failures

A new category for 2021 focuses on making assumptions related to software updates, critical data, and CI/CD pipelines without verifying integrity.

Notable Common Weakness Enumerations (CWEs) include CWE-829: Inclusion of Functionality from Untrusted Control Sphere, CWE-494: Download of Code Without Integrity Check, and CWE-502: Deserialization of Untrusted Data.

List of Mapped CWEs

- **CWE-345 Insufficient Verification of Data Authenticity**
- **CWE-353 Missing Support for Integrity Check**
- **CWE-426 Untrusted Search Path**
- **CWE-494 Download of Code Without Integrity Check**
- **CWE-502 Deserialization of Untrusted Data**
- **CWE-565 Reliance on Cookies without Validation and Integrity Checking**

- **CWE-784 Reliance on Cookies without Validation and Integrity Checking in a Security Decision**
- **CWE-829 Inclusion of Functionality from Untrusted Control Sphere**
- **CWE-830 Inclusion of Web Functionality from an Untrusted Source**
- **CWE-915 Improperly Controlled Modification of Dynamically-Determined Object Attributes**



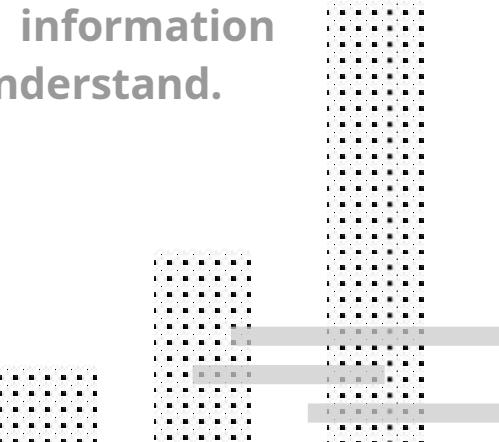

Insecure De-serialization

Serialization

Serialisation is the process of converting objects used in programming into simpler, compatible formatting for transmitting between systems or networks for further processing or storage

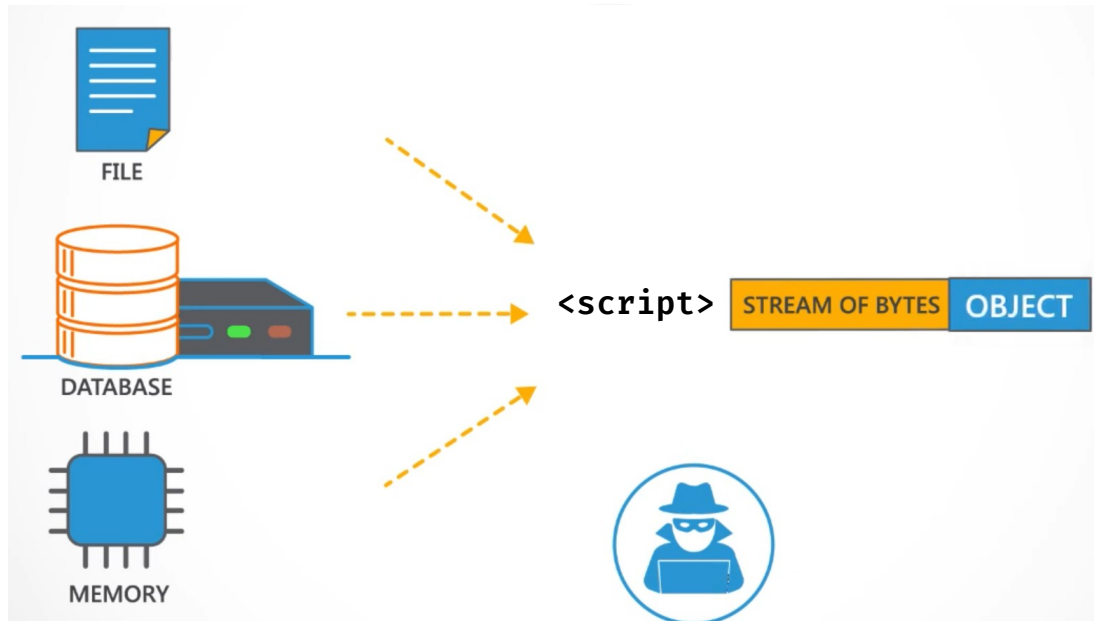
De-serialization

De-serialisation is the reverse of this; converting serialised information into their complex form - an object that the application will understand.



Insecure De-serialization

Insecure de-serialization occurs when untrusted data is used to abuse the logic flow of an application.





Insecure De-serialization



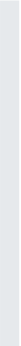
Demo



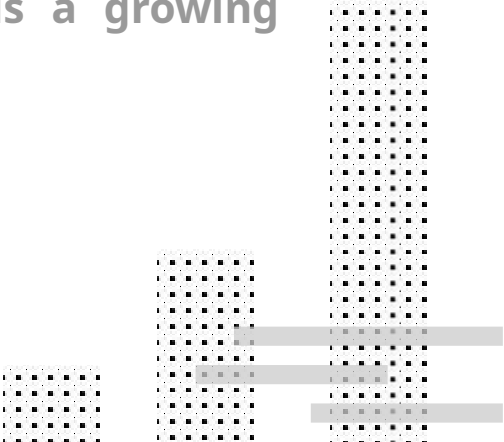
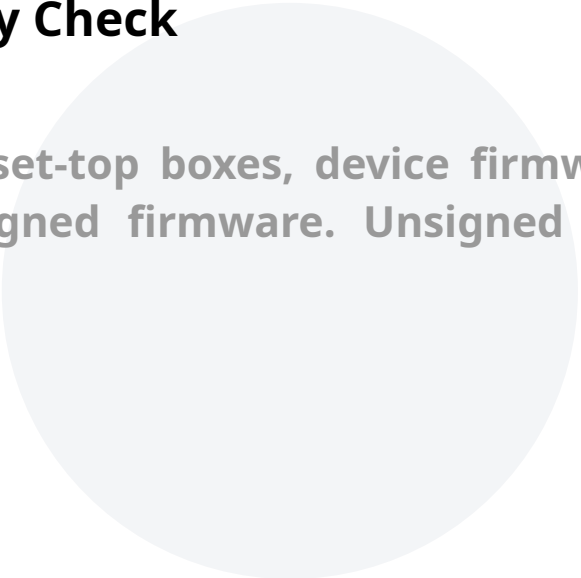


Update without signing

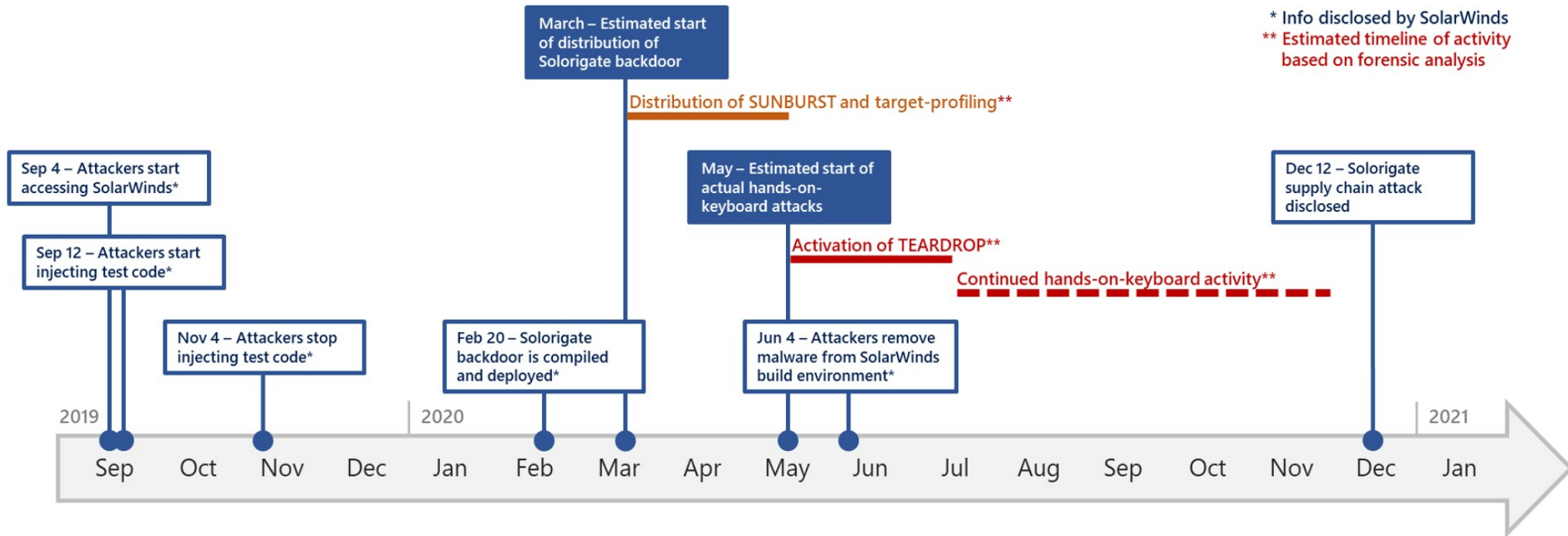
CWE-345 Insufficient Verification of Data Authenticity | CWE-353 Missing Support for Integrity Check



Many home routers, set-top boxes, device firmware, and others do not verify updates via signed firmware. Unsigned firmware is a growing target for attackers



Solarwinds Hack



Mitigations

- Use digital signatures or similar mechanisms to verify the software or data is from the expected source and has not been altered.
- Ensure libraries and dependencies, such as npm or Maven, are consuming trusted repositories.
- Ensure that there is a review process for code and configuration changes to minimize the chance that malicious code or configuration could be introduced into your software pipeline.
- Ensure that unsigned or unencrypted serialized data is not sent to untrusted clients without some form of integrity check or digital signature to detect tampering or replay of the serialized data

Further reading resources & links

“ Scan :



Thanks!
Any Questions ?

”