# CWE Detail – CWE-611

## Description

The product processes an XML document that can contain XML entities with URIs that resolve to documents outside of the intended sphere of control, causing the product to embed incorrect documents into its output.

## Extended Description

XML documents optionally contain a Document Type Definition (DTD), which, among other features, enables the definition of XML entities. It is possible to define an entity by providing a substitution string in the form of a URI. The XML parser can access the contents of this URI and embed these contents back into the XML document for further processing. By submitting an XML file that defines an external entity with a file:// URI, an attacker can cause the processing application to read the contents of a local file. For example, a URI such as "file:///c:/winnt/win.ini" designates (in Windows) the file C:\Winnt\win.ini, or file:///etc/passwd designates the password file in Unix-based systems. Using URIs with other schemes such as http://, the attacker can force the application to make outgoing requests to servers that the attacker cannot reach directly, which can be used to bypass firewall restrictions or hide the source of attacks such as port scanning. Once the content of the URI is read, it is fed back into the application that is processing the XML. This application may echo back the data (e.g. in an error message), thereby exposing the file contents.

## Threat-Mapped Scoring

Score: 3.25

Priority: P2 - Serious (High)

## Observed Examples (CVEs)

**•** CVE-2022-42745: Recruiter software allows reading arbitrary files using XXE

**•** CVE-2005-1306: A browser control can allow remote attackers to determine the existence of files via Javascript containing XML script.

**•** CVE-2012-5656: XXE during SVG image conversion

**•** CVE-2012-2239: XXE in PHP application allows reading the application's configuration file.

**•** CVE-2012-3489: XXE in database server

**•** CVE-2012-4399: XXE in rapid web application development framework allows reading arbitrary files.

**•** CVE-2012-3363: XXE via XML-RPC request.

**•** CVE-2012-0037: XXE in office document product using RDF.

**•** CVE-2011-4107: XXE in web-based administration tool for database.

**•** CVE-2010-3322: XXE in product that performs large-scale data analysis.

**•** CVE-2009-1699: XXE in XSL stylesheet functionality in a common library used by some web browsers.

## Related Attack Patterns (CAPEC)

* CAPEC-221

## Modes of Introduction

**•** Implementation: REALIZATION: This weakness is caused during implementation of an architectural security tactic.

## Common Consequences

**•** Impact: Read Application Data, Read Files or Directories — Notes: If the attacker is able to include a crafted DTD and a default entity resolver is enabled, the attacker may be able to access arbitrary files on the system.

**•** Impact: Bypass Protection Mechanism — Notes: The DTD may include arbitrary HTTP requests that the server may execute. This could lead to other attacks leveraging the server's trust relationship with other entities.

**•** Impact: DoS: Resource Consumption (CPU), DoS: Resource Consumption (Memory) — Notes: The product could consume excessive CPU cycles or memory using a URI that points to a large file, or a device that always returns data such as /dev/random. Alternately, the URI could reference a file that contains many nested or recursive entity references to further slow down parsing.

## Potential Mitigations

**•** Implementation: Many XML parsers and validators can be configured to disable external entity expansion. (Effectiveness: N/A)

## Applicable Platforms

**•** XML (Class: None, Prevalence: Undetermined)

## Notes

**•** Relationship: CWE-918 (SSRF) and CWE-611 (XXE) are closely related, because they both involve web-related technologies and can launch outbound requests to unexpected destinations. However, XXE can be performed client-side, or in other contexts in which the software is not acting directly as a server, so the "Server" portion of the SSRF acronym does not necessarily apply.