APACHECON
DENVER
WESTIN DENVER DOWNTOWN
APRIL 7-9, 2014

Security best practices for Apache web services

Presented For The Apache Foundation By
LINUX FOUNDATION

Agenda

- Security Advisories @ Apache
- Issues associated with the advisory process
- Apache CXF advisories + lessons learned
- Closing remarks

Speaker Introduction

Apache CXF

Apache Syncope

talend*
*open data solutions

Apache Santuario

Apache Webservices

Security Advisories @ Apache

A Flaw is Discovered…

- Someone discovers a security flaw in an Apache project
- That someone could be a security researcher who has done extensive analysis of the codebase.
- Or it could be an end-user who is puzzled about the output of a particular configuration or use-case.
- Or it could be an Apache developer who suddenly realises that some part of the project is not behaving as it should.

Reporting the Issue

- How the issue is reported to the project tends to vary according to the type of discoverer.
- A security researcher will typically know to alert only a security expert associated with a project, or mail private/security@<project>.apache.org
- An Apache developer may just alert private@ also, or may keep it secret until it has been fixed.
- Non-Apache users/developers may not know the proper procedure for reporting the issue.

Verifying the Issue

- The first step is to verify that the security issue exists
- The next step is typically to write a test-case to reproduce the issue (can also help in verification of this issue).
- The project informs the discoverer of their conclusion + discuss/agree a possible fix
- The project alerts security@apache.org + receives a CVE number.

Fixing the Issue

- The issue is fixed (possibly with a somewhat misleading or vague commit message).
- If the fix is complex or environment-specific, the issue reporter may be asked to validate the fix locally.
- The project team backports the fix to all active branches of the project (if applicable)
- The security team of the project drafts a CVE advisory, briefly describing the flaw, versions affected, the commit in which it was fixed, and the project versions that are fixed

Releasing the Fix

- The Apache project releases versions which contain the fix for the advisory.
- The advisories are signed and typically then uploaded to a special “advisories” page on the project website.
- Example: http://cxf.apache.org/security-advisories.html
- The advisories are publicized via the project mailing lists, as well as various third-party security lists.

Issues associated with the advisory process

Premature Disclosure

- An end user may unwittingly publish the issue via logging a JIRA or some queries to a users@<project>.apache.org list.
- Example: CVE-2013-0239: Authentication bypass in the case of WS-SecurityPolicy enabled plaintext UsernameTokens.
- Was reported first in JIRA as issue CXF-4776: UsernameTokenValidator do not validate that password is not provided.

Premature Disclosure II

- Moderation of Apache mailing lists / JIRA not possible
- However we can change JIRA issues to only be seen by committers / PMC members
- Mitigate mailing list disclosures by taking any further comment “off-line”.
- Properly document reporting procedure for security issues on the project website.

Release timing

- Once an issue is fixed, the project must decide when to perform the next release
- A critical bug may warrant immediate release
- If other issues are in the works, a release may be delayed to avoid a drip-feed of security advisories
- Commercial factors may also come into play

Disclosure timing

- Once a release takes place, the project must decide when to release the advisory
- Normal practice is to disclose the advisory shortly after the release takes place
- It may be delayed to allow users time to upgrade
- The timing may also depend on external factors

Disagreements

- Disagreements can arise in a number of areas
- The issue reporter may not agree with the fix
- Developers may disagree on release timing
- There can be issues with back porting fixes
- A robust PMC will greatly help with these problems

APACHECON
DENVER
WESTIN DENVER DOWNTOWN
APRIL 7-9, 2014

Apache CXF advisories + lessons learned

Presented For The Apache Foundation By
LINUX FOUNDATION

Supporting edge-cases

- CVE-2013-0239: http://cxf.apache.org/cve-2013-0239.html
- Authentication bypass if a WS-Security UsernameToken element is sent with no password child element, when using WS-SecurityPolicy
- Root cause was to support deriving keys from UsernameTokens for signature
- Make sure supporting “edge-cases” doesn't weaken security!

Beware legacy features

- CVE-2012-5633: http://cxf.apache.org/cve-2012-5633.html
- Bypass of WS-Security processing if a HTTP GET request is issued to a service URL
- Caused by a legacy interceptor that allows some basic "rest style" access to a simple SOAP service.
- Don't be afraid to remove legacy features when releasing new major versions!

Write negative tests

- CVE-2012-0803: http://cxf.apache.org/cve-2012-0803.html
- WS-Security Username Tokens not validated properly against the required policies.
- A malicious client could send a request to the endpoint with no UsernameToken, and the UsernameToken policy requirement would still be marked as valid!
- A negative test run as part of an automated process would have caught this.
- Good idea to review specs periodically - “what would happen if I sent the following message to...”

Avoid weak algorithms

- CVE-2011-2487: http://cxf.apache.org/note-on-cve-2011-2487.html
- Exploits a weakness of the PKCS#1 v1.5 public key encryption scheme
- Can be used to recover a symmetric encryption key
- Define what algorithms are acceptable (signature, encryption, etc.) + abort before processing a non-compliant algorithm.
- WS-SecurityPolicy is perfect for this.

Beware timing attacks

- Previous vulnerability essentially involved a timing attack on CXF/WSS4J
- In WS-Security, a symmetric key encrypts the payload, and is in turn encrypted by an asymmetric (public) key (typically)
- An adversary could conduct a timing attack to see whether an exception was thrown during the decryption of the symmetric key or not
- Solution was to generate a temporary key if this happened, making it harder to see when processing failed.

Beware old standards

- CVE-2011-1096: http://cxf.apache.org/note-on-cve-2011-1096.html
- Describes an attack on XML Encryption using CBC mode
- An adversary can use this to completely decrypt an encrypted request
- However, WS-SecurityPolicy specification does not define any “non-CBC” mode AlgorithmSuites!
- CXF introduced “custom” AlgorithmSuite values that use GCM mode – however, this is not interoperable.

Beware DoS attacks

- CVE-2013-2160: Denial of Service Attacks on Apache CXF
- Various XML-based attacks: Huge number of Elements/Attributes, deeply nested XML tree, hash collision attacks.
- The fix was to have configurable values for the above associated with the StAX XML parser (Woodstox).
- Use automated tools to see if your endpoints/stack is vulnerable!

Beware of Spoofing

- CVE-2012-3451: SOAP Action spoofing attack - http://cxf.apache.org/cve-2012-3451.html
- Possible to execute other web service operation by spoofing SOAP Action
- CVE-2013-2172: Java XML Signature spoofing attack
- Exploited a weakness in algorithm constraints for XML Signature “Canonicalization Method”.

Beware of XML!

- CVE-2010-2076: http://svn.apache.org/repos/asf/cxf/trunk/security/CVE-2010-2076.pdf
- CXF processed Document Type Declarations (DTDs) in certain scenarios.
- CVE-2013-4517: http://santuario.apache.org/secadv.data/cve-2013-4517.txt.asc
- XML Signature DoS attacks based on allowing DTDs for transformations.
- Many other issues involve allowing XSLT/XPath

APACHECON
DENVER
WESTIN DENVER DOWNTOWN
APRIL 7-9, 2014

Closing remarks

Presented For The Apache Foundation By
LINUX FOUNDATION

Encourage openness

- The prompt + transparent handling of security advisories promotes confidence in a project
- Avoid excessive secrecy or the temptation not to disclose a vulnerability
- Having said that, no need to give “too much” information on how to reproduce an attack.
- It is also a good thing to build a relationship with security researchers / analysts

Questions

APACHECON DENVER
WESTIN DENVER DOWNTOWN
APRIL 7-9, 2014

Presented For The Apache Foundation By
LINUX FOUNDATION