Koordinierungsstelle
für IT-Standards

OSCI-Transport Bibliothek: Schwachstelle ermöglicht das Ausspähen von Daten

Versionierung

Version	Beschreibung	Status	Datum
1.0	Dokument erstellt	Final	22.06.2017

Zusammenfassung

Ein entfernter Angreifer kann unter den folgenden Voraussetzungen zwei Schwachstellen ausnutzen, um Systeminformationen auszuspähen und diese für weitere Angriffe zu verwenden:

1) Der Angreifer hat Zugriff auf einen Verzeichnisdienst einer OSCI-Infrastruktur.
2) Die OSCI-Nachrichten werden vom Empfänger nach einer optionalen Absenderauthentifizierung angenommen und verarbeitet.

Die Schwachstellen basieren auf der Verarbeitung externer Entitäten in OSCI-Nachrichten sowie der Durchführung einer Padding-Oracle-Attack innerhalb der OSCI-Infrastruktur. Ein sicherer Betrieb der OSCI-Infrastruktur verringert die Auswirkungen der Angriffe und erschwert die Ausführung der Angriffe.

Ein Sicherheitsupdate für Hersteller ist im Update der OSCI-Transport Bibliothek auf die Versionen 1.7.1 (Java) sowie 1.7 (.NET) enthalten:

1. OSCI Transport Bibliothek 1.7.1 in Java
2. OSCI Transport Bibliothek 1.7 in .NET
3. Informationen zum Update: OSCI-Transport 1.2 - Korrigenda 03/2017

Die vorliegende Sicherheitsempfehlung ist verfügbar unter: http://www.xoev.de/de/download

Betroffene Produkte

In der OSCI-Infrastruktur sind folgende Komponenten betroffen:

- OSCI-Client (in der OSCI-Spezifikation: aktiver Empfänger),
- OSCI-Backend (in der OSCI-Spezifikation: passiver Empfänger).

Betroffen sind alle Produkte, in denen die OSCI-Transport Bibliothek in der Version 1.6. (.NET) / 1.6.1. (JAVA) oder kleiner eingesetzt wird.

Nicht betroffen sind Produkte, in denen die OSCI-Transport Bibliothek ab Version 1.7. (.NET) / 1.7.1. (JAVA) eingesetzt wird.

Aktualisierte Version der OSCI-Transport Bibliothek

Die KoSIT informiert über die Schwachstellen in der OSCI-Transport Bibliothek und stellt ein Sicherheitsupdate im Rahmen des Updates auf die Versionen 1.7.1 (Java) sowie 1.7 (.NET) zur Verfügung.

Die KoSIT empfiehlt die umgehende Verwendung der Versionen 1.7.1 (Java) sowie 1.7 (.NET) in der Entwicklung von Produkten für die OSCI-Infrastruktur.

Informationen zu den Schwachstellen

Die Schwachstellen basieren auf der Verarbeitung externer Entitäten in OSCI-Nachrichten sowie der Durchführung einer Padding-Oracle-Attack innerhalb der OSCI-Infrastruktur. Ein grundlegend sicherer Betrieb der OSCI-Infrastruktur wirkt schadensverringernd und angriffserschwerend.

Voraussetzung für die Ausnutzung der Schwachstellen ist der Versand standardkonformer Nachrichten. Für den Versand von OSCI-Nachrichten innerhalb einer OSCI-Infrastruktur sind gültige, aktuelle Informationen aus einem Verzeichnisdienst dieser OSCI-Infrastruktur erforderlich, die nur authentifizierten Nutzern zur Verfügung gestellt werden. Für den Empfang und die Verarbeitung von OSCI-Nachrichten ist entscheidend, ob diese nur von authentifizierten Absendern akzeptiert werden oder auch teilweise von nicht-authentifizierten Absendern.

Zur XXE Schwachstelle

Wenn die genannten Angriffsvoraussetzungen erfüllt sind, lassen sich Daten aus dem System des OSCI-Clients bzw. -Backends ausspähen, die für weitere Angriffe verwendet werden können.

Die KoSIT empfiehlt, zusätzlich zum Update ausschließlich Nachrichten von authentifizierten Absendern anzunehmen. Die KoSIT empfiehlt zudem unter Verwendung der verfügbaren Verzeichnisdienste Nachrichten sowohl auf Fach- wie auch auf Transportebene zu signieren und zu verschlüsseln.

Zur Padding-Oracle-Attack

Der OSCI-Client ist von dieser Schwachstelle nicht betroffen.

Zusätzlich zu den oben geschilderten Voraussetzungen muss der Angreifer in der OSCI-Infrastruktur die Position eines Man-in-the-Middle einnehmen. Der Angriff kann nur auf kryptografische Verfahren mit Cipher-Block Chaining (CBC-Modus) durchgeführt werden.

Wenn diese Voraussetzungen erfüllt sind, kann die Verschlüsselung der Transportdaten aufgehoben werden.

Die Durchführung einer Padding-Oracle-Attack auf kryptografische Verfahren mit CBC-Modus wird verhindert, wenn im Betrieb der Systeme die Empfehlungen der Technischen Richtlinie BSI TR-02102-1 zu Paddingverfahren allgemein und zum CBC-Modus insbesondere beachtet werden.

Die KoSIT empfiehlt, die Vorgaben der technischen Richtlinie für den sicheren Einsatz des CBC-Modus zu beachten:

- BSI TR-02102-1 Version 2017-01 mit Stand vom 08. Februar 2017: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.pdf

Die KoSIT empfiehlt zusätzlich zum Update zeitnah die Ablösung des CBC-Modus durch den GCM-Modus (Galois/Counter-Modus). Auch für den Einsatz des GCM-Modus sind die Empfehlungen der Technischen Richtlinien und Standards des BSI zu beachten.

Auf der Padding-Oracle-Attack aufbauende XML Signature Wrapping Attack

Voraussetzung für den Angriff ist, dass ein Angreifer Zugriff auf unverschlüsselte Transportdaten (Transportnachricht) oder auf darin unverschlüsselte Fachnachrichten hat. Zusätzlich darf eine Nachricht nicht auf mehrfach auftretende Elemente, insbesondere nicht auf eine doppelte Verwendung von XML-IDs überprüft werden. Die so manipulierte Nachricht muss jedoch in der weiteren Verarbeitung trotz doppelter Elemente oder XML-IDs von den Fach- und Transportverfahren korrekt verarbeitet werden können. Der KoSIT sind keine OSCI-Infrastrukturen bekannt, in denen eine korrekte Weiterverarbeitung so manipulierter Nachrichten erfolgt.

Sind diese zusätzlichen Voraussetzungen erfüllt, kann ein Angreifer die jeweilige Nachricht verändern, ohne eine vorhandene Signatur zu kompromittieren (XML Signature Wrapping Attack).

Die KoSIT empfiehlt den Herstellern von Fach-und Transportverfahren, Nachrichten auf mehrfach auftretende Elemente und insbesondere auf eine doppelte Verwendung von XML-IDs zu prüfen.

Risikoabschätzung

Die Risikoabschätzung der Schwachstelle erfolgt unter Verwendung des Klassifizierungsschemas für Schwachstellen des CERT-Bund (https://cert-bund.de/risk).

Das Eintrittspotential ist „mittel“. Die Schwachstellen sind ausnutzbar, da für die dargestellten Sicherheitslücken Proof of Concepts existieren (XXE, XML Signature Wrapping, Padding Oracle). Es gibt keine Anzeichen dafür, dass die Schwachstellen bereits ausgenutzt werden. Eine Ausnutzung der Schwachstelle kann prinzipiell automatisiert erfolgen, jedoch nicht selbstreplizierend.

Das Schadenspotential ist „mittel“. Die Auswirkungen eine Ausnutzung der Schwachstellen führt zu einem Abfluss von Informationen über das betroffene System (OSCI-Client, OSCI-Backend), die Integrität des Systems ist nicht betroffen und die Angriffe führen weder zu einer Übernahme der Kontrolle noch zur einer Übernahme von Berechtigungen. Die beschriebenen Angriffe wirken sich nicht auf das gesamte Netzwerk aus. Da Fachnachrichten entsprechend ihrem Schutzniveau und getrennt von der OSCI-Nachricht signiert und verschlüsselt werden, sind diese weiterhin angemessen geschützt und von den beschriebenen Angriffen nicht betroffen.

Das aktuelle Schadenspotential ist „mittel“, es ergibt sich aus dem mittleren Eintritts- und dem mittleren Schadenspotential.

Vorfälle und Bekanntmachungen

Der KoSIT sind keine öffentlichen Bekanntmachungen oder Sicherheitsvorfälle bekannt, welche die in dieser Sicherheitsempfehlung beschriebenen Schwachstellen betreffen.

Quelle

Ausgangspunkt für die Sicherheitsempfehlung der KoSIT sind die Ergebnisse eines Tests der Firma SEC Consult und darauf aufbauende Prüfungen der Firma Governikus, die der KoSIT zur Verfügung gestellt wurden. Wir bedanken uns insbesondere bei der Firma SEC Consult für die Entdeckung und die Unterstützung einer koordinierten Schwachstellenveröffentlichung. Desweiteren danken wir der Firma Governikus für die schnelle und umfassende Prüfung.