OSCI-Transport Bibliothek: Schwachstelle ermöglicht das Ausspähen von Informationen

Versionierung

Version	Beschreibung	Status	Datum
0.1	Dokument erstellt	Entwurf	14.01.2019
0.2	Dokument überarbeitet	Entwurf	24.01.2019
0.3	Überarbeitung mit Kommentaren von SEC Consult	Entwurf	30.01.2019

Zusammenfassung

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

1) Die OSCI-Nachrichten werden vom Empfänger nach einer optionalen Absenderauthentifizierung angenommen und verarbeitet.

Die Schwachstellen basieren auf der Verarbeitung von signaturrelevanten Elementen in OSCI-Nachrichten sowie der Durchführung einer Oracle-Attacke 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 1.8.3 (Java und .NET) enthalten:

1. OSCI Transport Bibliothek 1.8.3 in Java
2. OSCI Transport Bibliothek 1.8.3 in .NET

Die vorliegende Sicherheitsempfehlung ist verfügbar unter:
https://www.xoev.de/sixcms/media.php/13/OSCI12_SecurityAdvisory_20190205.pdf.

Betroffene Produkte

In der OSCI-Infrastruktur sind folgende Komponenten betroffen:

- OSCI-Backend (in der OSCI-Spezifikation: passiver Empfänger).
- OSCI-Manager (Intermediär)

Betroffen sind alle Produkte, in denen die OSCI-Transport Bibliothek in der Version 1.8 (.NET) / 1.8.1 (JAVA) oder kleiner eingesetzt wird.

Nicht betroffen sind Produkte, in denen die OSCI-Transport Bibliothek ab Version 1.8.3 (Java und .NET) 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 1.8.3 (Java und .NET) zur Verfügung.

Die KoSIT empfiehlt die umgehende Verwendung der Version 1.8.3 (Java und .NET) in der Entwicklung von Produkten für die OSCI-Infrastruktur.

Informationen zu den Schwachstellen

Die Schwachstellen basieren auf der Verarbeitung von signaturrelevanten Elementen in OSCI-Nachrichten sowie der Durchführung einer Oracle-Attacke 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. Authentifiziert wird hier an Hand der Signatur der Inhaltsdaten, die verschlüsselt für den Leser übermittelt werden. Auf diese Daten hat keine am OSCI-Transport beteiligte Komponente Zugriff.

Zur Schwachstelle „Unsicheres kryptographisches Verfahren“

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.

Auf Grund der generellen Schwachstellenproblematik des CBC-Modus ist davon auszugehen, dass weitere Angriffsszenarien auf die OSCI-Infrastruktur wahrscheinlich sind. Deswegen werden die folgenden zwei Empfehlungen gegeben:

Die KoSIT empfiehlt die Verwendung von AES-GCM. Auch für den Einsatz des GC-Modus sind die Empfehlungen der Technischen Richtlinien und Standards des BSI zu beachten.

Sofern weiterhin AES-CBC verwendet wird, empfiehlt die KoSIT zusätzlich den Einsatz von TLS.

Zur Schwachstelle „Signaturumgehung“

Zusätzlich zu den oben geschilderten Voraussetzungen, muss ein Angreifer Zugriff auf die unverschlüsselten Transportdaten einer Nachricht haben. Ist diese zusätzliche Voraussetzung erfüllt, kann ein Angreifer die jeweilige Nachricht verändern, ohne eine vorhandene Signatur zu kompromittieren.

Die KoSIT empfiehlt, zusätzlich zum Update ausschließlich Nachrichten von authentifizierten Absendern anzunehmen.

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 diese Proof of Concepts existieren (Oracle, Signature Bypass). 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 „gering“. Die Auswirkungen eine Ausnutzung der Schwachstellen führt zu einem Abfluss von Informationen über eine Nachrichtenübermittlung eines Nutzers, der AES-CBC einsetzt. Die Integrität des Dienstes oder 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 die innerhalb von OSCI-Nachrichten transportierten 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 „gering“, dies ergibt sich aus dem mittleren Eintritts- und dem geringe 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 bei der Firma SEC Consult für die Unterstützung einer verantwortungsbewussten Veröffentlichung und insbesondere bei der Firma Governikus für die schnelle und umfassende Prüfung.