ANALIZIRANJE RANJIVOSTI

Dependency: dom4j – 2.1.1

Ranjivosti: dom4j dozvoljava eksterne DTD-ove (Document Type Definition) I entitete, što može omogućiti XXE napade.

XXE napad je tip napada na aplikaciju koja parsira ulazne XML podatke. Ovaj napad se događa kada je nepoverljiv ulazni XML koji sadrži referencu na spoljašnji entitet, procesuiran od strane slabo konfigurisanog XML parsera.

Napadi mogu uključiti otkrivanje lokalnih fajlova koji mogu sadržati privatne korisničke podatke, onemogućavanje usluge kao I SSRF (Server Side Request Forgery) napade preko kojih se mogu, nepoželjno, menjati resursi na serveru. Podrazumevana podešavanja za većinu Java XML parsera je da imaju omogućen XXE. Kako bismo koristili ove parsere bezbedno moramo eksplicitno isključiti XXE u istim.

Rešenje zavisi od konkretnog izbora XML procesora, zato što svaka implementacija ima svoj način procesuiranja eksterne šeme I DTD-ova. Konkretno, za ovaj dependency može se iskoristiti Open SUSE Security update pomoću kog se rešava XXE ranjivost u SAX parserima.

Dependency: guava-16.0

Ranjivosti: Korišćenjem klasa poput AtomicDoubleArray I CompoundOrdering koje se dobavljaju iz ovog dependency-ja pojavljuje se ranjivost u vidu neograničene alokacije memorije.

Napadač može da pošalje veliki broj zahteva sa velikom količinom podataka koje će server čitati bez provere. Ovo može dovesti do zauzimanja celokupne serverske memorije.

Rešenje podrazumeva prelazak na noviju verziju dependency-ja u kojoj je ova ranjivost razrešena. Verzija: guava-25.0

Dependency: Log4j

Ranjivosti: Nepravilna validacija sertifikata hosta u Apache Log4j SMTP (Simple Mail Transfer Protocol) appendera.

“Man-in-the-middle” napadač bi mogao presresti SMTPS konekciju I na taj način bi mogli biti otkriveni log zapisi appendera.

Rešenje podrazumeva prelazak na noviju verziju dependency-ja u kojoj je ova ranjivost razrešena. Verzija: Log4j-2.13.2, ili više.

Dependency: spring-security-core-5.2.2

Ranjivosti: Unutar ovog dependency-ja postoje ranjivosti vezane za kriptografiju.

Može se desiti da je Spring Security inicijalizovan null vektorom u implementaciji tekst enkriptora. Maliciozan korisnik sa pristupom podacima koji su enkriptovani korišćenjem takvog enkriptora može pristupiti dekriptovanim vrednostima korišnjenjem “dictionary” napada.

Rešenje podrazumeva prelazak na noviju verziju dependency-ja u kojoj je ova ranjivost razrešena. Verzija: spring-security-core-5.3.2

Dependency: tomcat-embed-core-9.0.33

Ranjivosti: Kada koristimo ovu verziju dependency-ja napadač može da kontroliše sadržaj I ime datoteke na serveru, server je konfigurisan da koristi PersistenceManager sa FileStore-om, postoji dovoljno propustljiv filter koji omogućava napadaču da pročita objekat I napadač poznaje relativnu putanju datoteke za skladištenje koju FileStore koristi I nad kojim napadač ima kontrolu. Da bi napad uspeo svi navedeni uslovi moraju biti ispunjeni.

Rešenje podrazumeva prelazak na noviju verziju dependency-ja u kojoj je ova ranjivost razrešena. Verzija: tomcat-embed-core-9.0.36