Computer Emergency Response Team

BOLLETTINO IT-CERT.180823.B01
Vulnerabilità critica in Apache Struts 2
(CVE-2018-11776)

MINISTERO DELLO
SVILUPPO ECONOMICO

DESCRIZIONE

Apache Software Foundation Struts è un *framework* open source utilizzato per la creazione di applicazioni Web Java.

È stata scoperta una vulnerabilità critica (CVE-2018-11776) in Apache Struts versione 2.x che potrebbe consentire ad un attaccante di eseguire codice arbitrario da remoto.

La vulnerabilità si manifesta nei casi in cui il risultato di un'azione definito in un file di configurazione XML (*tag* `<result>`) non specifica il valore `namespace` e, allo stesso tempo, le azioni di livello superiore nella stessa configurazione non hanno il valore `namespace` specificato o contengono un valore di tipo *wildcard*.

La vulnerabilità è presente anche nel caso in cui un risultato punta ad una pagina JSP *template* che a sua volta contiene un *tag* di tipo URL (`<s:url>`) e l'azione corrispondente non specifica il valore `namespace` o contiene un valore *wildcard*.

Un attaccante potrebbe sfruttare questa vulnerabilità inviando ad un'applicazione affetta una richiesta HTTP contenente un parametro `namespace` appositamente predisposto che non viene correttamente validato dal *framework* Struts. Se sfruttata con successo, questa vulnerabilità potrebbe consentire all' attaccante di eseguire codice arbitrario nel contesto dell'applicazione affetta.

Al momento non ci sono notizie che questa vulnerabilità sia stata sfruttata in attacchi reali.

Sono disponibili aggiornamenti che risolvono questa vulnerabilità nelle versioni affette di Apache Struts 2. È altresì disponibile una soluzione alternativa per mitigare questa vulnerabilità (per maggiori informazioni si veda la sezione LINK UTILI).

SOLUZIONE

Aggiornare Apache Struts 2 alla versione 2.3.35 o alla versione 2.5.17, dopo appropriato *testing*.

In alternativa, è possibile applicare la soluzione di mitigazione suggerita dal produttore nel relativo bollettino di sicurezza (si veda la sezione LINK UTILI).

SISTEMI

Risultano affette dalla vulnerabilità oggetto di questo bollettino le seguenti versioni di Apache Struts:

- Apache Struts dalla versione 2.3 alla 2.3.34
- Apache Struts dalla versione 2.5 alla 2.5.16

Altre versioni non supportate di questo prodotto potrebbero risultare vulnerabili.

La vulnerabilità è presente nel codice *core* di Apache Struts. Tutte le applicazioni che utilizzano Struts risultano potenzialmente vulnerabili.

LINK UTILI

Avviso del produttore

https://cwiki.apache.org/confluence/display/WW/S2-057

Semmle

https://semmle.com/news/apache-struts-CVE-2018-11776

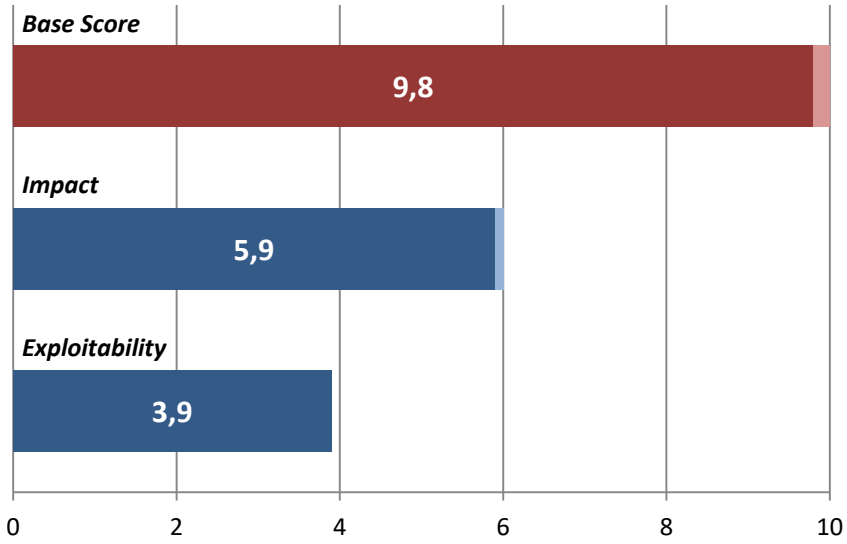
lgtm

https://lgtm.com/blog/apache_struts_CVE-2018-11776

Mitre CVE ID

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-11776

VALUTAZIONE CVSS



Relativamente alla valutazione della *severity* come metrica di base - da intendersi quale livello di pericolosità della vulnerabilità delle componenti di sistema o delle piattaforme - il CERT Nazionale valuta i parametri che concorrono al calcolo della *Base Score* secondo lo standard CVSS v3 (*Common Vulnerabilities Scoring System*), avvalendosi del *tool* messo a disposizione dal sito del NIST (https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator).

Nello specifico, sulla base di informazioni preliminari soggette ad aggiornamento, sono stati raggiunti i seguenti punteggi:

- *Base Score:* 9,8
- *Impact:* 5,9
- *Exploitability:* 3,9

Vettore CVSS: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

NOTE

Le informazioni contenute nel presente bollettino sono fornite a meri fini informativi.

In nessun caso il CERT Nazionale può essere ritenuto responsabile di qualunque perdita, pregiudizio, responsabilità, costo, onere o spesa, ivi comprese le eventuali spese legali, danno diretto, indiretto, incidentale o consequenziale, derivante da o connesso alle informazioni riportate nel presente bollettino.

La versione PDF del bollettino è statica ed, in quanto tale, contiene le informazioni disponibili al momento della pubblicazione.