Computer Emergency Response Team

BOLLETTINO IT-CERT.181016.B01

Vulnerabilità critica in IBM WebSphere Application Server (CVE-2018-1567)

MINISTERO DELLO
SVILUPPO ECONOMICO

DESCRIZIONE

WebSphere Application Server (WAS) è una piattaforma *middleware* (*application server*) prodotta da IBM che consente di eseguire applicazioni Web sviluppate in Java.

È stata scoperta una vulnerabilità critica (CVE-2018-1567) in IBM WAS che può causare l'esecuzione di codice arbitrario da remoto.

La vulnerabilità può consentire ad un attaccante remoto di eseguire codice Java arbitrario mediante un oggetto serializzato appositamente predisposto inviato attraverso il connettore SOAP (*Simple Object Access Protocol*) da una sorgente non fidata.

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

IBM ha rilasciato aggiornamenti software che risolvono la vulnerabilità nei prodotti affetti (per maggiori informazioni si veda la sezione LINK UTILI).

SOLUZIONE

Il produttore raccomanda di applicare al più presto ad ogni prodotto vulnerabile la rispettiva *Interim Fix*, il *Fix Pack* o il pacchetto PTF contenente l'APAR PH03986.

Per maggiori informazioni sui prodotti vulnerabili e sugli aggiornamenti disponibili, incluse istruzioni per l'installazione, si raccomanda di consultare la documentazione online elencata nella sezione LINK UTILI.

SISTEMI

Risultano affette dalla vulnerabilità descritta in questo bollettino le seguenti versioni di IBM WebSphere Application Server (WAS) e WAS Hypervisor Edition:

- IBM WAS dalla versione 9.0.0.0 alla 9.0.0.9
- IBM WAS dalla versione 8.5.0.0 alla 8.5.5.14
- IBM WAS dalla versione 8.0.0.0 alla 8.0.0.15
- IBM WAS dalla versione 7.0.0.0 alla 7.0.0.45

LINK UTILI

Bollettino di sicurezza IBM

https://www-01.ibm.com/support/docview.wss?uid=swg22016254

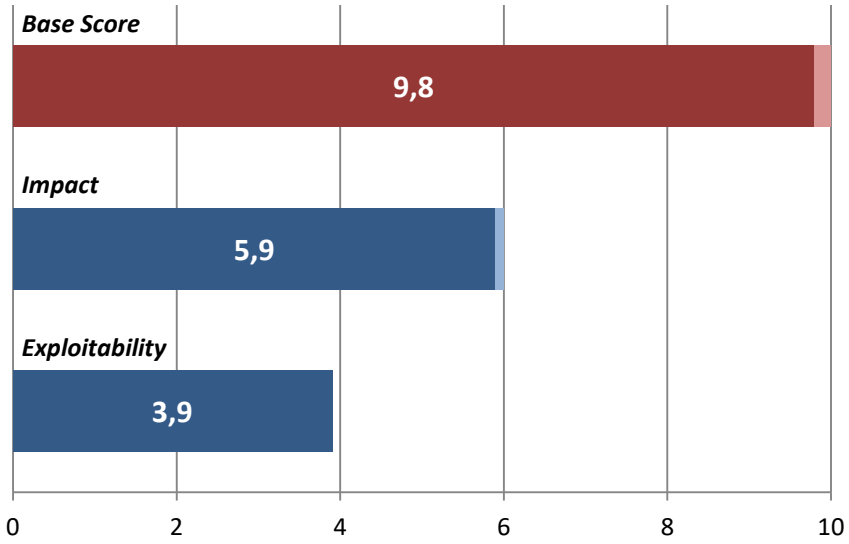
IBM PH03986

http://www-01.ibm.com/support/docview.wss?uid=ibm10732515

Mitre CVE ID

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-1567

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.