



**Computer Emergency Response Team**

**BOLLETTINO IT-CERT.190527.B01**  
**Vulnerabilità critica in IBM WebSphere**  
**Application Server**  
**(CVE-2019-4279)**



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-2019-4279) in IBM WAS che può consentire l'esecuzione di codice arbitrario da remoto.

La vulnerabilità può essere sfruttata mediante l'invio da sorgenti non fidate di una sequenza appositamente predisposta di oggetti serializzati. Se sfruttata con successo, questa vulnerabilità può consentire all'attaccante di eseguire codice arbitrario da remoto nel contesto dell'applicazione affetta. A seconda dei privilegi associati all'applicazione, l'attaccante potrebbe essere in grado di installare programmi, visualizzare, modificare o eliminare dati o creare nuovi account con diritti utente completi. Tentativi non riusciti di sfruttare questa vulnerabilità potrebbero causare condizioni di *denial of service*.

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 la rispettiva *Interim Fix*, il *Fix Pack* o il pacchetto PTF contenente l'APAR corrispondente ad ogni specifica versione del prodotto affetta dalla vulnerabilità oggetto di questo bollettino.

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):

- WebSphere Application Server ND Version 9.0
- WebSphere Application Server ND Version 8.5
- WebSphere Virtual Enterprise Version 7.0

## LINK UTILI

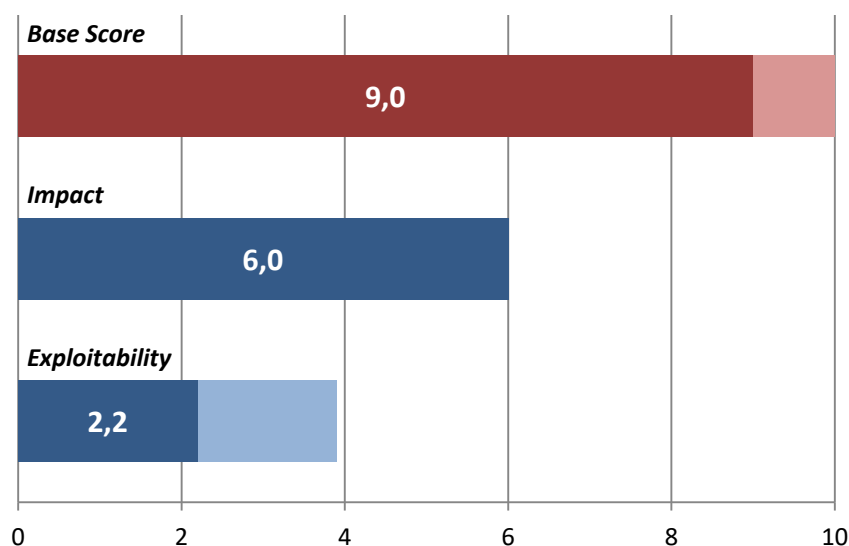
### **Bollettino di sicurezza IBM**

<https://www-01.ibm.com/support/docview.wss?uid=ibm10883628>

### **Mitre CVE ID**

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-4279>

## 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 sono stati raggiunti i seguenti punteggi:

- *Base Score*: 9,0
- *Impact*: 6,0
- *Exploitability*: 2,2

Vettore CVSS 3.0: AV:N/AC:H/PR:N/UI:N/S:C/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.