CVE-2025-34067

Produs Afectat	Hikvision Integrated Security Management Platform (HikCentral/applyCT component)
Endpoint vulnerabil	**/bic/ssoService/v1/applyCT**
Scor CVSS	10 (CRITIC)
CWE	• CWE-502 (Deserializare de date necontrolate) • CWE-917 (Expression Language Injection)
Descriere	• Apare din cauza folosirii unei versiuni vulnerabile a bibliotecii *Fastjson*, care activează caracteristica periculoasă "auto-type" fără verificări adecvate. • Endpoint-ul permit deserializarea *JSON* manipulat, încărcând clase Java arbitrare, exemplu ***JdbcRowSetImpl*** de pe un server *LDAP* controlat de atacator
Metodele de exploatare	Atacatorii pot exploata această vulnerabilitate prin trimiterea unei cereri *POST* special create, cu un payload *JSON* malițios, care instruiește sistemul să deserializeze o clasă *Java* (cum ar fi ***JdbcRowSetImpl***) de pe un server *LDAP* la distanță controlat de atacator. Aceasta permite declanșarea funcției ***auto-type*** a *Fastjson* și execuția de cod arbitrar pe sistemul subiacent fără autentificare sau interacțiune cu utilizatorul.
Impact potențial	• Execuție la distanță de cod, fără autentificare. • Control complet asupra serverului ***Hikvision***, inclusiv acces la fluxuri video, manipulări fizice, sau mișcări laterale. • Reprezintă un risc major de securitate cibernetică și fizică, afectând infrastructuri sensibile.
Măsuri de remediere	• Izolarea ***endpoint***-ului vulnerabil (***/bic/ssoService/v1/applyCT***) de pe zonele accesibile din internet. • Monitorizarea traficului ***LDAP*** de la sistemele ***Hikvision***, pentru detectarea posibilelor atacuri. • Dezactivarea funcției auto-type din ***Fastjson*** dacă este posibil. • Rămâne critică disponibilizarea unei actualizări oficiale de către ***Hikvision*** pentru ***Fastjson*** sau platformă. • Urmărește paginile comerciale/parteneri și canalele oficiale ***Hikvision*** pentru lansarea patch-urilor.
IoCs	• Indicatori în trafic: ➢ Cereri HTTP POST către ***/bic/ssoService/v1/applyCT*** cu content JSON ce include: ✓ Cheia ***"@type"*** sau clase Java cunoscute (ex: com.sun.rowset.JdbcRowSetImpl, org.apache.commons.beanutils.BeanComparator). ✓ Referințe LDAP (***ldap://*** sau ***rmi://).*** • Jurnale / Fișiere: ✓ Loguri suspecte în HikCentral logs (de ex. hikcentral.log) care includ accesări de tip: ***„POST /bic/ssoService/v1/applyCT HTTP/1.1*** ***Host: x.x.x.x*** ***Content-Type: application/json”***
Referință	https://nvd.nist.gov/vuln/detail/CVE-2025-34067

	https://github.com/advisories/GHSA-ch97-xgvh-p6mh https://vulners.com/cve/CVE-2025-34067 https://radar.offseq.com/threat/cve-2025-34067-cwe-502-deserialization-of-untruste-475dc43e https://securityonline.info/critical-hikvision-applyct-flaw-cve-2025-34067-cvss-10-0-unauthenticated-rce-via-fastjson/