DOKUMENT JE ELEKTRONSKO PODPISAN!
Podpisnik: Borut Jakopin
Izdajatelj certifikata: SI-PASS-CA
Številka certifikata: 36AD8B6B000000005756C7F3
Potek veljavnosti: 18. 10. 2029
Čas podpisa: 18. 11. 2026 13:17
Št. dokumenta: 386-70/2026-1544-3

REPUBLIKA SLOVENIJA
URAD VLADE RS ZA INFORMACIJSKO VARNOST

Ulica gledališča BTC 2, 1000 Ljubljana

T: 01 478 4778
E: gp.uiv@gov.si
W: http://www.uiv.gov.si
X: @URSIV_Slovenia

Številka: 386-70/2026-1544-3
Datum: 18. 11. 2026

Na podlagi devetega odstavka 37. člena Zakona o informacijski varnosti (Uradni list RS, št. 40/25; v nadaljnjem besedilu: ZInfV-1) in ocene ogroženosti z dne 21. oktobra 2026, s katero je bila ogroženost ovrednotena kot visoka, Urad Vlade Republike Slovenije za informacijsko varnost (v nadaljnjem besedilu: URSIV) kot pristojni nacionalni organ iz prvega odstavka 10. člena ZInfV-1 izdaja naslednjo

O D R E D B O

o izvedbi nujnih ukrepov v zvezi z kritično ranljivostjo Java4Shell (CVE-2026-114938) v izvajalnih okoljih Java

Za nižanje ocene visoke ogroženosti ter posledično preprečitev nastanka krize se odreja izvedba nujnih ukrepov pri zavezancih po ZInfV-1 (v nadaljnjem besedilu: naslovniki). S to odredbo se določajo vrsta in obseg del, ki jih je treba opraviti pri navedenih subjektih, ter roki za njihovo izvedbo. Kadar omrežje ali informacijski sistem naslovnika upravlja drug subjekt, naslovnik ukrepe izvede v sodelovanju z upravljavcem oziroma ga nemudoma pozove k njihovi izvedbi.

I. Identifikacija

Naslovniki identificirajo aplikacije ter omrežne in informacijske sisteme, ki uporabljajo izvajalna okolja Java, vključno z OpenJDK in distribucijami, ki temeljijo na njem. Pregled zajema strežnike, navidezne stroje, vsebnike, slike vsebnikov ter aplikacije in naprave z lastnim oziroma vgrajenim izvajalnim okoljem Java (JRE ali JDK).

Za vsako namestitev ugotovijo proizvajalca oziroma distribucijo, celotno oznako različice in gradnje dejansko uporabljenega izvajalnega okolja, procesorsko arhitekturo, razpoložljivost ukazov AVX-512 VBMI ter zagonske nastavitve navideznega stroja Java (JVM). Prizadetost ugotavljajo na podlagi distribucije in različice izvajalnega okolja, procesorske podpore AVX-512 VBMI ter obvestil proizvajalca o prizadetosti izdelka. Podatek, ali aplikacija neposredno ali prek knjižnic dekodira podatke Base64 iz nezaupanja vrednih virov, uporabijo le za določitev prednosti, ne za izključitev prizadetosti. Pri navideznih strojih in vsebnikih podporo AVX-512 VBMI preverijo za vse gostitelje oziroma vozlišča, na katerih se lahko zaženejo, saj JVM razpoložljive ukaze procesorja zazna ob vsakem zagonu.

Prednostno preverijo internetno dostopne aplikacije in storitve za upravljanje identitet ter avtentikacijo, zlasti Keycloak. Preverijo tudi namestitve Jira, Confluence, Jenkins, JFrog

Artifactory in PingFederate, če jih uporabljajo. Sama prisotnost navedenega izdelka še ne pomeni, da so izpolnjeni pogoji za izrabo ranljivosti.

Če prizadetosti v roku za identifikacijo ni mogoče zanesljivo izključiti, namestitev do zaključka preverjanja obravnavajo kot potencialno prizadeto in zanjo izvedejo zaščitne ukrepe iz III. točke.

Rok za izvedbo: 24 ur od vročitve te odredbo.

II. Namestitev popravkov

Naslovniki v prizadetih namestitvah namestijo podprto različico izvajalnega okolja Java, ki po navedbah njegovega proizvajalca oziroma vzdrževalca odpravlja CVE-2026-114938. Za Oracle JDK v vejah 17, 21, 25 in 27 so to različice, novejše od tistih, ki jih Oracle v varnostnem obvestilu navaja kot prizadete (17.0.21.0.3, 21.0.13.0.3, 25.0.5.0.3 in 27.0.1.0.3). Za Oracle Java SE 8-perf in Oracle GraalVM uporabijo ustrezno posodobitev iz varnostnega obvestila proizvajalca. Pri drugih distribucijah uporabijo njihove popravljene pakete. Oznake popravljenih različic se lahko razlikujejo.

Pri izdelkih z vgrajenim izvajalnim okoljem Java uporabijo način posodobitve, ki ga podpira proizvajalec izdelka. Če popravek še ni na voljo, od proizvajalca zahtevajo informacijo o prizadetosti, začasnih ukrepih in predvidenem roku izdaje posodobitve ter do njene namestitve izvajajo ukrepe iz III. točke.

Po posodobitvi ponovno zaženejo vse prizadete procese JVM oziroma ponovno vzpostavijo vsebnike iz posodobljenih slik. Preverijo, da vsak aplikacijski proces dejansko uporablja popravljeno izvajalno okolje, in preverijo pravilno delovanje storitev. Sama posodobitev operacijskega sistema ali privzete sistemske Jave ne zadošča, če aplikacije uporabljajo drugo izvajalno okolje. Posodobitve pridobijo izključno iz uradnih virov proizvajalca oziroma vzdrževalca in pred namestitvijo preverijo njihovo celovitost. Pred posodobitvijo zagotovijo možnost povrnitve v prejšnje delujoče stanje.

Rok za izvedbo: 48 ur od vročitve te odredbe za internetno dostopne aplikacije in sisteme ter sedem dni od vročitve za druge aplikacije in sisteme. Če popravek za uporabljeno distribucijo oziroma izdelek ob seznanitvi še ni na voljo, navedeni rok začne teči z njegovo razpoložljivostjo. Do namestitve popravka je obvezno izvajanje ukrepov iz III. točke.

III. Ukrepi kadar takojšnja namestitev popravkov ni mogoča

Kadar takojšnja namestitev popravkov ni mogoča, naslovniki nemudoma ocenijo tveganje in po predhodnem preverjanju združljivosti ter vpliva na delovanje v zagonsko konfiguracijo vsakega prizadetega procesa JVM dodajo parameter:

-XX:-UseBASE64Intrinsics

S tem izključijo optimizirano izvajanje dekodiranja Base64, ki vsebuje ranljivo programsko pot. Po spremembi ponovno zaženejo prizadete procese JVM ter preverijo, da je parameter pri vseh procesih dejansko uveljavljen in da storitve pravilno delujejo. Uveljavitev preverijo pri tekočem procesu, na primer z ukazom jcmd <PID> VM.flags -all. Parameter dodajo le prizadetim procesom JVM, saj se JVM, ki parametra ne prepozna, ne zažene. Če ga nastavijo prek okoljske spremenljivke (na primer JAVA_TOOL_OPTIONS), upoštevajo, da velja za vse JVM, zagnane v tem okolju. Nastavitev vključijo tudi v konfiguracije za samodejni zagon, ponovno ustvarjanje vsebnikov in nove namestitve. Pri vgrajenih izvajalnih okoljih upoštevajo navodila proizvajalca izdelka.

Do namestitve popravkov dostop do izpostavljenih storitev omejijo na nujne uporabnike in sisteme, kolikor to dopušča zagotavljanje nujnih storitev. Če izključitve ranljive programske poti ni mogoče izvesti ali njene učinkovitosti ni mogoče potrditi, aplikacije oziroma sisteme do izvedbe učinkovitega ukrepa izolirajo od javnih omrežij in omejijo tudi druge poti, po katerih bi lahko napadalec posredoval podatke ranljivi aplikaciji. Pri tem upoštevajo tudi odhodne povezave, saj je po navedbah raziskovalcev ranljivost mogoče izrabiti tudi, ko se aplikacija Java poveže na zlonameren strežnik.

Začasni ukrepi ne nadomeščajo namestitve popravkov. Po uspešni posodobitvi o nadaljnji uporabi začasne nastavitve odločijo na podlagi navodil proizvajalca in preverjanja delovanja.

Rok za izvedbo: nemudoma po ugotovitvi, da takojšnja namestitev popravkov ni mogoča, najpozneje pa v 24 urah od te ugotovitve. Ukrepi se izvajajo do preverjene namestitve popravkov.

IV. Prizadete različice brez podpore

Za prizadete namestitve, za katere redni varnostni popravki niso več zagotovljeni, naslovniki namestijo popravek ponudnika podaljšane podpore ali izvajalno okolje oziroma izdelek nadgradijo na podprto in popravljeno različico. Do takrat izvajajo ukrepe iz III. točke. Če učinkovitega začasnega ukrepa ni mogoče zagotoviti, sistem izolirajo od javnih omrežij in drugih nezaupanja vrednih virov podatkov.

Rok za izvedbo: enak kot v II. točki, za začasne ukrepe velja rok iz III. točke.

V. Spremljanje in preverjanje znakov izkoriščanja

Naslovniki spremljajo varnostna obvestila proizvajalcev in vzdrževalcev izvajalnih okolij Java, proizvajalcev uporabljene programske opreme ter pristojne skupine CSIRT. Na prizadetih oziroma potencialno prizadetih sistemih preverijo morebitne znake poskusov izkoriščanja ali kompromitacije, zlasti:

- nepričakovana sesutja JVM, ponavljajoče se ponovne zagone ter neobičajne napake pri obdelavi podatkov Base64;
- nepričakovane procese, ukaze, datoteke ali omrežne povezave, ki izvirajo iz aplikacijskega procesa Java;
- nepooblaščene spremembe aplikacij, uporabniških računov ali nastavitev ter neobičajno uporabo avtentikacijskih žetonov.

Zavarujejo relevantne sistemske, aplikacijske, avtentikacijske in omrežne dnevnike ter zapise o sesutjih pred izgubo ali prepisom. Pri ravnanju z izpisi pomnilnika upoštevajo, da lahko vsebujejo občutljive podatke. Ob zaznani kompromitaciji izvedejo odzivne ukrepe v sodelovanju s pristojno skupino CSIRT. Po potrebi prekličejo izpostavljene žetone in zamenjajo kompromitirane poverilnice. Odsotnost znakov kompromitacije ne odpravlja obveznosti posodobitve. Javno objavljenih dokazov koncepta (PoC) ne izvajajo na produkcijskih sistemih, saj lahko povzročijo sesutje JVM in poškodbo podatkov.

Rok za izvedbo: začetno preverjanje v 48 urah od vročitve te odredbe, nato sprotno spremljanje do izvedbe vseh ukrepov.

VI. Priglasitev incidentov

Naslovniki, za katere velja obveznost priglasitve, pomembne incidente priglasijo pristojni skupini CSIRT v skladu s 30. členom ZInfV-1 in v tam določenih rokih. Za prostovoljno priglasitev

incidentov, kibernetskih groženj in skorajšnjih incidentov se uporablja 35. člen ZInfV-1. To pomeni, da naslovniki na SIGOV-CERT (cert@gov.si) priglasijo incidente subjekti javne uprave na državni[1] in lokalni ravni[2] ter ponudniki storitev zaupanja, ki jih izvajajo subjekti državne uprave. Na SI-CERT (cert@cert.si) priglasijo incidente zavezanci, ki niso v pristojnosti SIGOV-CERT. Subjekti, ki niso zavezanci po ZInfV-1, lahko priglasijo incident SI-CERT, njihova priglasitev pa se obravnava kot prostovoljna.

VII. Poročanje

O izvedbi ukrepov od I. do V. točke naslovniki poročajo pristojni skupini CSIRT iz prejšnje točke. Naslovniki poročajo na naslov in v obliki, kot ju določa ta odredba.

Rok za izvedbo: 72 ur od vročitve te odredbe, nato ob vsaki spremembi stanja do izvedbe vseh ukrepov.

VIII. Nadzor

Nadzor nad izvršitvijo te odredbe izvajajo inšpektorji za informacijsko varnost v skladu s prvim odstavkom 45. člena ZInfV-1.

[1] Subjekti javne uprave na državni ravni so ministrstva, organi v njihovi sestavi, vladne službe in upravne enote ter tisti javni infrastrukturni zavodi, ki so ustanovljeni v skladu z zakonom, ki ureja znanstvenoraziskovalno in inovacijsko dejavnost. Mednje spadajo tudi drugi subjekti javne uprave iz Priloge 3, ki je kot Priloga sestavni del ZInfV-1.

[2] Subjekti javne uprave na lokalni ravni so občine. Konkretno gre za mestne občine kot je opredeljeno v Prilogi 2, ki je kot Priloga sestavni del ZInfV-1.

Obrazložitev

URSIV je zaradi nenadne spremembe varnostnih razmer, povezane z ranljivostjo Java4Shell (CVE-2026-114938) in ocene visoke ogroženosti kibernetske varnosti v Republiki Sloveniji in izdal odredbo o izvedbi nujnih ukrepov v zvezi z kritično ranljivostjo Java4Shell (CVE-2026-114938) v izvajalnih okoljih Java.

Raziskovalci podjetja Calif so 17. novembra 2026 razkrili ranljivost v optimiziranem dekodirniku Base64 v OpenJDK. Ranljivost je po oceni Calif po CVSS 4.0 ocenjena z 9,2, Oracle pa zanjo navaja oceno 8,1 po CVSS 3.1. Nujnost ukrepanja poleg ocen CVSS temelji na navedbi proizvajalca Oracle, da lahko napadalec brez avtentikacije prek omrežja doseže prevzem izvajalnega okolja, ter na možnih posledicah.

Pri obdelavi posebej pripravljenih podatkov Base64 lahko optimizirana rutina JVM, ki uporablja ukaze AVX-512 VBMI, napačno izračuna dolžino podatkov in povzroči zapis zunaj dodeljenega območja pomnilniške kopice. Naknadno zaznana nepravilnost ne prepreči že nastale poškodbe pomnilnika. Po ugotovitvah raziskovalcev lahko ustrezna priprava razporeditve objektov na kopici omogoči razkritje vsebine pomnilnika in oddaljeno izvajanje kode s pravicami aplikacijskega procesa. Med možnimi posledicami so razkritje gesel, ključev in avtentikacijskih žetonov, nedelovanje storitev ter prevzem nadzora nad aplikacijo.

Calif navaja, da je v testnih okoljih prikazal izvajanje kode brez predhodne avtentikacije pri privzetih konfiguracijah izdelkov Keycloak, Jira, Confluence, Jenkins, JFrog Artifactory in PingFederate. Navedeno ne pomeni, da so ranljive vse namestitve teh izdelkov. Prizadetost je odvisna od uporabljene distribucije in različice Jave, strojne opreme, nastavitev JVM ter od tega, ali aplikacija napadalcu omogoča posredovanje podatkov ranljivemu dekodirniku. Zaradi vloge storitev za upravljanje identitet lahko kompromitacija takšne aplikacije vpliva tudi na varnost povezanih storitev.

Ranljiva programska pot je prisotna v OpenJDK od različice 17.0.6 dalje do ustreznih popravljenih izdaj ter v distribucijah, ki jo vključujejo. Oracle med prizadetimi izdelki posebej navaja tudi določeno izdajo Java SE 8-perf in izdaje Oracle GraalVM. Standardni izvajalni okolji Java 8 in 11 ranljive programske poti ne vsebujeta. Zato je treba prizadetost presojati po celotni oznaki izdelka in gradnje ter po obvestilih njegovega proizvajalca. Izraba obravnavane programske poti zahteva okolje x86-64 z razpoložljivo podporo AVX-512 VBMI. Sistemi ARM64 po objavljenih informacijah niso prizadeti zaradi te ranljivosti.

Oracle je 17. novembra 2026 izdal varnostne posodobitve. Pri drugih distribucijah in izdelkih z vgrajeno Javo je treba spremljati njihove proizvajalce ter uporabiti ustrezen popravek. Inventarizacija in preverjanje dejansko zagnanih izvajalnih okolij sta nujna, saj lahko na istem sistemu obstaja več neodvisnih namestitev Jave. Posodobitev ene namestitve ne odpravi ranljivosti drugih namestitev ali že zagnanih procesov.

Do posodobitve je mogoče z izključitvijo optimiziranega dekodirnika Base64 preprečiti uporabo ranljive programske poti. Ukrep zahteva ustrezno zagonsko nastavitev, ponovni zagon vseh prizadetih procesov ter preverjanje njene uveljavitve. Ker začasna konfiguracija ne odstrani ranljive kode in jo lahko poznejša namestitev ali ponovni zagon brez te nastavitve ponovno izpostavi, ostaja namestitev popravka obvezna.

Prikaz izrabe v testnem okolju sam po sebi ni dokaz zlonamernega izkoriščanja pri naslovnikih ali v Republiki Sloveniji. Vendar javno razkritje ranljivosti, prikazana možnost izrabe brez predhodne avtentikacije in možne posledice za podatke ter povezane storitve utemeljujejo hitro preventivno ukrepanje tudi brez potrjenega incidenta.

Navedene okoliščine ob ugotovljeni visoki ogroženosti utemeljujejo izdajo odredbe za nižanje ocene ogroženosti in preprečitev nastanka krize. URSIV na podlagi devetega odstavka 37. člena ZInfV-1 odreja nujne ukrepe ter določa njihov obseg in roke. Prednostna obravnava internetno dostopnih sistemov, možnost začasne zaščite in roki, ki upoštevajo razpoložljivost popravkov proizvajalcev, omogočajo sorazmerno izvedbo ukrepov. Ukrepi so glede na pogoje izrabe ranljivosti in možne škodljive posledice potrebni za dosego namena odredbe.

Borut Jakopin
namestnik v. d. direktorja urada