

ODGOVORNO PRIJAVLJIVANJE SIGURNOSNIH RANJIVOSTI

Pronašli ste ranjivost? Prijavite je odgovorno.

Kako prijaviti sumnju na sigurnosne ranjivosti u ITO proizvodima, uslugama i digitalnoj infrastrukturi.

ID DOKUMENTA

ITO-TRUST-VDP-001

VERZIJA

1.0

KLASIFIKACIJA

JAVNO

VLASNIK DOKUMENTA

Informacijska
sigurnost

CIKLUS REVIZIJE

Godišnje

NA SNAZI OD

Listopad 2026.

Jasan kanal za sigurnosne prijave

ITO je predan održavanju sigurnosti svojih softverskih proizvoda, usluga i digitalne infrastrukture.

Unatoč pažljivom inženjeringu, sigurnosnom testiranju i stalnom održavanju, ranjivosti se i dalje mogu otkriti.

Cijenimo odgovorno sigurnosno istraživanje i potičemo sigurnosne istraživače, korisnike, partnere i druge strane da ITO-u prijave sumnju na sigurnosne ranjivosti postupkom opisanim u ovoj politici.

Naš je cilj osigurati **jasan i odgovoran kanal** za prijavu mogućih sigurnosnih problema kako bi se mogli istražiti i, gdje je potrebno, otkloniti.

SADRŽAJ

01	Svrha	02
02	Kako prijaviti	03
03	Opseg	04
04	Odgovorno istraživanje	05
05	Nedopuštene aktivnosti	05
06	Nakon prijave	06
07	Rokovi odgovora	06
08	Koordinirano otkrivanje	07
09	Okruženja korisnika	07
10	Tehnologije trećih strana	08
11	Privatnost prijava	08
12	Priznanje	08
13	Kontakt	09

UKRATKO

PRIJAVA NA
security@ito.dev

NASLOV E-
POŠTE
**SECURITY
VULNERABILITY
REPORT**

SUSTAVI KORISNIKA
**Nisu odobreni za
testiranje**

VRSTA
PROGRAMA
**Program
otkrivanja, nije
bug bounty**

KONTROLA DOKUMENTA

ID DOKUMENTA	ITO-TRUST-VDP-001
VERZIJA	1.0
KLASIFIKACIJA	JAVNO
VLASNIK	Informacijska sigurnost
CIKLUS REVIZIJE	Godišnje
NA SNAZI OD	Listopad 2026.

Pošaljite prijavu sigurnosnom timu

SUMNJU NA SIGURNOSNE RANJIVOSTI PRIJAVITE NA

security@ito.dev

NASLOV E-POŠTE, GDJE JE MOGUĆE **SECURITY VULNERABILITY REPORT**

Informacije koje treba navesti

Kako bismo lakše razumjeli i istražili prijavu, molimo navedite što više relevantnih informacija koliko je to razumno moguće, uključujući:

01 Pogođeni proizvod, uslugu ili URL

02 Opis sumnje na ranjivost

03 Korake potrebne za reprodukciju problema

04 Mogući sigurnosni utjecaj

05 Relevantne snimke zaslona, zapise ili tehničke informacije

06 Materijal za dokaz koncepta potreban za razumijevanje problema



Molimo ne uključujte osobne, povjerljive ili operativno osjetljive informacije, osim ako su nužne za objašnjenje ranjivosti.

Sustavi obuhvaćeni ovom politikom

Ova se politika odnosi na javno dostupne sustave u vlasništvu ITO-a i kojima upravlja ITO, a koji su izričito navedeni kao dio opsega ovog programa otkrivanja ranjivosti.

U OPSEGU OVLAŠTENOG TESTIRANJA

Izričito navedeni ITO sustavi

Javno dostupni sustavi u vlasništvu ITO-a i kojima upravlja ITO, izričito navedeni kao dio opsega ovog programa.

NIJE AUTOMATSKI U OPSEGU

ITO softver u okruženjima korisnika

ITO softver implementiran u okruženjima pod kontrolom korisnika nije automatski uključen u opseg ovlaštenog sigurnosnog testiranja prema ovoj politici.

Sigurnosni problemi otkriveni u ITO proizvodima implementiranim u okruženjima korisnika i dalje se mogu prijaviti ITO-u, ali istraživači ne smiju testirati sustave korisnika bez izričitog ovlaštenja organizacije odgovorne za te sustave.



Ova politika ne daje dopuštenje za testiranje sustava kojima upravljaju korisnici ITO-a.

Postupajte odgovorno i u dobroj vjeri

TIJEKOM ISTRAŽIVANJA MOLIMO

- ✓ Izbjegavajte pristup informacijama izvan onoga što je razumno potrebno za dokazivanje problema
- ✓ Izbjegavajte mijenjanje ili brisanje informacija
- ✓ Izbjegavajte ometanje sustava ili usluga
- ✓ Izbjegavajte smanjenje dostupnosti ili performansi sustava
- ✓ Izbjegavajte pristup računima drugih korisnika
- ✓ Izbjegavajte društveni inženjering, phishing ili testiranje fizičke sigurnosti
- ✓ Prekinite testiranje ako nenamjerno pristupite osjetljivim, osobnim ili operativnim informacijama
- ✓ Prijavite ranjivost ITO-u što je prije razumno moguće

Cilj treba biti dokazati postojanje moguće ranjivosti uz **najmanju nužnu interakciju** s pogođenim sustavom.

ISTRAŽIVAČI NE SMIJU NAMJERNO PROVODITI

- ✗ Napade uskraćivanjem usluge ili iscrpljivanjem resursa
- ✗ Destruktivno testiranje
- ✗ Postavljanje zlonamjernog softvera
- ✗ Društveni inženjering
- ✗ Phishing
- ✗ Krađu vjerodajnica
- ✗ Fizički upad
- ✗ Namjerni pristup računima trećih strana
- ✗ Nepotrebno izvlačenje podataka
- ✗ Mijenjanje ili brisanje produkcijskih informacija
- ✗ Testiranje infrastrukture korisnika bez ovlaštenja

Automatizirano skeniranje ranjivosti koje stvara značajan promet, degradaciju usluge ili operativni rizik također je izvan predviđenog opsega ove politike.

Naš postupak

Kada ITO zaprimi prijavu ranjivosti, naš postupak može uključivati:

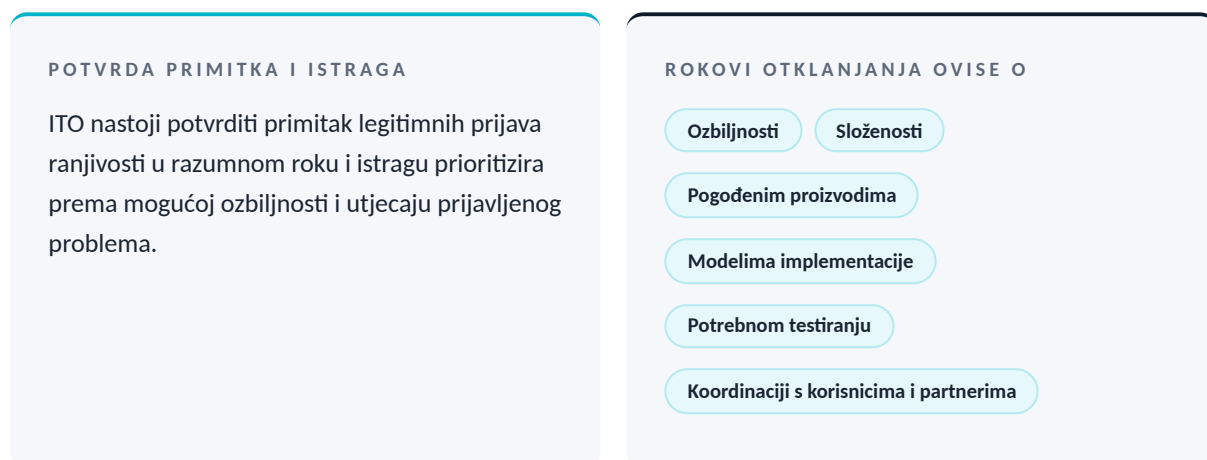


ITO će ULOŽITI RAZUMNE NAPORE DA



07 • ROKOVI ODGOVORA

Prioritet prema ozbiljnosti i utjecaju



Objavljujemo zajedno, ne prerano

Molimo istraživače da javno ne objavljuju pojedinosti o ranjivosti prije nego što ITO dobije razumnu priliku da je istraži i, gdje je potrebno, razvije i distribuira odgovarajuće otklanjanje.

ITO podržava odgovorno i koordinirano otkrivanje ranjivosti s ciljem zaštite pogođenih korisnika i organizacija, uz priznavanje doprinosa legitimnog sigurnosnog istraživanja.

Kada je prikladno i uz dogovor s istraživačem, ITO može javno odati priznanje osobama koje odgovorno prijave sigurnosne ranjivosti.

Sustavi korisnika zahtijevaju ovlaštenje korisnika

ITO tehnologija može biti implementirana u infrastrukturi u vlasništvu ili pod upravljanjem državnih institucija, organizacija javne sigurnosti i drugih korisnika.



Ova politika ne daje ovlaštenje za pristup tim okruženjima, njihovo skeniranje, ispitivanje, testiranje ni bilo kakvu drugu interakciju s njima.

MOŽETE

Prijaviti ITO-u moguću ranjivost u ITO proizvodu, ako je otkrivena bez neovlaštenog testiranja.

POTREBNO OVLAŠTENJE

Kada istraga zahtijeva interakciju s okruženjem pod kontrolom korisnika, potrebno je pribaviti odgovarajuće ovlaštenje odgovorne organizacije.

Ranjivosti u proizvodima trećih strana

ITO proizvodi mogu integrirati tehnologije trećih strana ili o njima ovisiti. Ako prijavljena ranjivost potječe iz proizvoda treće strane, ITO se može, kada je prikladno, koordinirati s relevantnim pružateljem. Istraživači će možda morati slijediti i postupak otkrivanja ranjivosti koji je utvrdio odgovorni proizvođač treće strane.

ITO ne može dati ovlaštenje za testiranje sustava ili tehnologija koje ne posjeduje ili ne kontrolira.

Kako se postupa s informacijama iz prijave

SVRHA

Dostavljene informacije koristit će se u svrhu istrage i odgovora na prijavljeni sigurnosni problem.

MINIMIZACIJA

Istraživači trebaju izbjegavati slanje nepotrebnih osobnih podataka ili povjerljivih podataka trećih strana.

KOORDINACIJA

Kada istraga zahtijeva koordinaciju s pogođenim korisnicima ili pružateljima tehnologije, relevantne tehničke informacije možda će trebati podijeliti s tim stranama.

Program otkrivanja, a ne bug bounty

NIJE BUG BOUNTY

Ova je politika program otkrivanja ranjivosti i ne predstavlja bug bounty program. ITO ne jamči financijsku naknadu za dostavljene prijave ranjivosti, osim ako nije izričito drukčije dogovoreno.

PRIZNANJE

Kada je prikladno i uz pristanak istraživača, ITO može javno odati priznanje za odgovorne doprinose.



13 • KONTAKT

Prijavite sigurnosnu ranjivost.

SIGURNOSNI KONTAKT

security@ito.dev

NASLOV E-POŠTE, GDJE JE MOGUĆE **SECURITY VULNERABILITY REPORT**

Za opća pitanja podrške, pitanja o proizvodima ili teme koje nisu vezane uz sigurnost, molimo koristite odgovarajući ITO kanal podrške, a ne adresu za prijavu ranjivosti.

DOKUMENT

Politika odgovornog otkrivanja ranjivosti

ID • VERZIJA • KLASIFIKACIJA

ITO-TRUST-VDP-001 • 1.0 • JAVNO

VLASNIK • REVIZIJA • NA SNAZI

Informacijska sigurnost • Godišnje • Listopad 2026.

TRUST CENTER

ito.dev/en/trust-center

TVRTKA

IT Odjel Mostar d.o.o., Mostar, Bosna i Hercegovina