# CVE Detail – CVE-2021-21244

OneDev is an all-in-one devops platform. In OneDev before version 4.0.3, There is a vulnerability that enabled pre-auth server side template injection via Bean validation message tampering. Full details in the reference GHSA. This issue was fixed in 4.0.3 by disabling validation interpolation completely.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## EPSS

EPSS Score: N/A

Percentile: 0.58043

## CVSS Scoring

CVSS v3.1 Score: 10.0

Severity: CRITICAL

## Mapped CWE(s)

* CWE-74: Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')
* CWE-94: Improper Control of Generation of Code ('Code Injection')

## CAPEC(s)

* CAPEC-10: Buffer Overflow via Environment Variables
* CAPEC-101: Server Side Include (SSI) Injection
* CAPEC-105: HTTP Request Splitting
* CAPEC-108: Command Line Execution through SQL Injection
* CAPEC-120: Double Encoding
* CAPEC-13: Subverting Environment Variable Values
* CAPEC-135: Format String Injection
* CAPEC-14: Client-side Injection-induced Buffer Overflow
* CAPEC-24: Filter Failure through Buffer Overflow
* CAPEC-242: Code Injection
* CAPEC-250: XML Injection
* CAPEC-267: Leverage Alternate Encoding
* CAPEC-273: HTTP Response Smuggling
* CAPEC-28: Fuzzing
* CAPEC-3: Using Leading 'Ghost' Character Sequences to Bypass Input Filters
* CAPEC-34: HTTP Response Splitting
* CAPEC-35: Leverage Executable Code in Non-Executable Files
* CAPEC-42: MIME Conversion
* CAPEC-43: Exploiting Multiple Input Interpretation Layers
* CAPEC-45: Buffer Overflow via Symbolic Links
* CAPEC-46: Overflow Variables and Tags
* CAPEC-47: Buffer Overflow via Parameter Expansion
* CAPEC-51: Poison Web Service Registry
* CAPEC-52: Embedding NULL Bytes
* CAPEC-53: Postfix, Null Terminate, and Backslash
* CAPEC-6: Argument Injection
* CAPEC-64: Using Slashes and URL Encoding Combined to Bypass Validation Logic
* CAPEC-67: String Format Overflow in syslog()
* CAPEC-7: Blind SQL Injection
* CAPEC-71: Using Unicode Encoding to Bypass Validation Logic
* CAPEC-72: URL Encoding
* CAPEC-76: Manipulating Web Input to File System Calls
* CAPEC-77: Manipulating User-Controlled Variables
* CAPEC-78: Using Escaped Slashes in Alternate Encoding
* CAPEC-79: Using Slashes in Alternate Encoding
* CAPEC-8: Buffer Overflow in an API Call
* CAPEC-80: Using UTF-8 Encoding to Bypass Validation Logic
* CAPEC-83: XPath Injection
* CAPEC-84: XQuery Injection
* CAPEC-9: Buffer Overflow in Local Command-Line Utilities

## ATT&CK Techniques

* T1027.009: Embedded Payloads
* T1574.007: Path Interception by PATH Environment Variable
* T1574.006: Dynamic Linker Hijacking
* T1562.003: Impair Command History Logging
* T1564.009: Resource Forking
* T1027: Obfuscated Files or Information
* T1027.006: HTML Smuggling

## Used By (Actors/Tools)

* TrickBot (malware)
* EKANS (malware)
* Pikabot (malware)
* SynAck (malware)
* Bumblebee (malware)
* Amadey (malware)
* Orz (malware)
* NOKKI (malware)
* AvosLocker (malware)
* COATHANGER (malware)
* Sardonic (malware)
* Matryoshka (malware)
* Ecipekac (malware)
* AppleSeed (malware)
* BUSHWALK (malware)
* macOS.OSAMiner (malware)
* NETWIRE (malware)
* OLDBAIT (malware)
* EnvyScout (malware)
* Emotet (malware)
* TEARDROP (malware)
* DUSTTRAP (malware)
* Turian (malware)
* BADHATCH (malware)
* Action RAT (malware)
* DUSTPAN (malware)
* Gootloader (malware)
* PolyglotDuke (malware)
* Hildegard (malware)
* SombRAT (malware)
* Snip3 (malware)
* RegDuke (malware)
* Moneybird (malware)
* InvisiMole (malware)
* P.A.S. Webshell (malware)
* Keydnap (malware)
* Line Dancer (malware)
* Conti (malware)
* Raspberry Robin (malware)
* Diavol (malware)
* Siloscape (malware)
* IcedID (malware)
* Kazuar (malware)
* CHIMNEYSWEEP (malware)
* FatDuke (malware)
* DRATzarus (malware)
* SHOTPUT (malware)
* Avaddon (malware)
* Conficker (malware)
* Flagpro (malware)
* Green Lambert (malware)
* ISMInjector (malware)
* PUNCHBUGGY (malware)
* POSHSPY (malware)
* MiniDuke (malware)
* Anchor (malware)
* DarkTortilla (malware)
* ROKRAT (malware)
* CORESHELL (malware)
* PlugX (malware)
* MultiLayer Wiper (malware)
* Lumma Stealer (malware)
* DustySky (malware)
* Epic (malware)
* Cuba (malware)
* Clambling (malware)
* DarkGate (malware)
* SVCReady (malware)
* Carbanak (malware)
* XTunnel (malware)
* Hydraq (malware)
* Netwalker (malware)
* Saint Bot (malware)
* Bundlore (malware)
* SMOKEDHAM (malware)
* Uroburos (malware)
* Trojan.Karagany (malware)
* Shamoon (malware)
* BPFDoor (malware)
* OopsIE (malware)
* StreamEx (malware)
* BoxCaon (malware)
* NightClub (malware)
* SDBbot (malware)
* RTM (malware)
* SodaMaster (malware)
* StrelaStealer (malware)
* Drovorub (malware)
* Kobalos (malware)
* Ryuk (malware)
* Final1stspy (malware)
* FinFisher (malware)
* Cobalt Strike (malware)
* SUNBURST (malware)
* Valak (malware)
* Samurai (malware)
* PoisonIvy (malware)
* NanoCore (malware)
* TajMahal (malware)
* Daserf (malware)
* Carbon (malware)
* Pisloader (malware)
* Ramsay (malware)
* Pillowmint (malware)
* SUNSPOT (malware)
* BoomBox (malware)
* DEADEYE (malware)
* PUNCHTRACK (malware)
* InnaputRAT (malware)
* GrimAgent (malware)
* Lokibot (malware)
* PoetRAT (malware)
* CoinTicker (malware)
* Ebury (malware)
* Maze (malware)
* ComRAT (malware)
* PowerStallion (malware)
* JPIN (malware)
* HTTPBrowser (malware)
* XCSSET (malware)
* KillDisk (malware)
* AppleJeus (malware)
* SoreFang (malware)
* Industroyer (malware)
* Agent Tesla (malware)
* ECCENTRICBANDWAGON (malware)
* ShadowPad (malware)
* QakBot (malware)
* Hancitor (malware)
* jRAT (malware)
* Dridex (malware)
* OSX/Shlayer (malware)
* Denis (malware)
* DEADWOOD (malware)
* Comnie (malware)
* Dtrack (malware)
* H1N1 (malware)
* SLOWPULSE (malware)
* ADVSTORESHELL (malware)
* HiddenWasp (malware)
* Small Sieve (malware)
* ShimRatReporter (tool)
* Sliver (tool)
* SILENTTRINITY (tool)
* PowerSploit (tool)
* Empire (tool)
* CARROTBALL (tool)
* Brute Ratel C4 (tool)
* Remcos (tool)
* Out1 (tool)
* Imminent Monitor (tool)
* MCMD (tool)
* Invoke-PSImage (tool)
* ArcaneDoor (campaign)
* Lazarus Group (intrusion-set)
* Aquatic Panda (intrusion-set)
* Earth Lusca (intrusion-set)
* Sandworm Team (intrusion-set)
* TA577 (intrusion-set)
* Ke3chang (intrusion-set)
* APT29 (intrusion-set)
* 2016 Ukraine Electric Power Attack (campaign)
* APT38 (intrusion-set)
* BackdoorDiplomacy (intrusion-set)
* Kimsuky (intrusion-set)
* Mustang Panda (intrusion-set)
* APT37 (intrusion-set)
* APT41 (intrusion-set)
* GALLIUM (intrusion-set)
* C0015 (campaign)
* Rocke (intrusion-set)
* RedCurl (intrusion-set)
* C0021 (campaign)
* Windshift (intrusion-set)
* Gamaredon Group (intrusion-set)
* Sea Turtle (intrusion-set)
* Moonstone Sleet (intrusion-set)
* APT3 (intrusion-set)
* C0017 (campaign)
* APT-C-36 (intrusion-set)
* Gallmaker (intrusion-set)
* BlackOasis (intrusion-set)

## Affected Products

* cpe:2.3:a:onedev\_project:onedev:\*:\*:\*:\*:\*:\*:\*:\*