IZVESTAJ O RANJIVOSTI BIBLIOTEKA

AIRBNB-PROJECT

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| BIBLIOTEKA | VERZIJA | CVE ID | RANJIVOST | RESENJE |
| go-redis/redis | v6.15.9 | CVE-2023-41056  CVE-2022-3734  CVE-2016-2121 | 1.Redis is an in-memory database that persists on disk. Redis incorrectly handles resizing of memory buffers which can result in integer overflow that leads to heap overflow and potential remote code execution. This issue has been patched in version 7.0.15 and 7.2.4.  2. \*\* DISPUTED \*\* A vulnerability was found in a port or fork of Redis. It has been declared as critical. This vulnerability affects unknown code in the library C:/Program Files/Redis/dbghelp.dll. The manipulation leads to uncontrolled search path. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The real existence of this vulnerability is still doubted at the moment. The identifier of this vulnerability is VDB-212416. NOTE: The official Redis release is not affected. This issue might affect an unofficial fork or port on Windows only.  3. A permissions flaw was found in redis, which sets weak permissions on certain files and directories that could potentially contain sensitive information. A local, unprivileged user could possibly use this flaw to access unauthorized system information. | 1.Ažurirati na najnoviju verziju kako bi se očuvala bezbednost sistema.  2.Pratiti zvanične izvore i ažurirati Redis samo iz pouzdanih izvora kako bi se izbegle potencijalne pretnje.  3.Jačanje dozvola na odgovarajućim fajlovima i direktorijumima u Redis instalaciji. Pravilna konfiguracija dozvola je ključna za očuvanje sigurnosti sistema. |
| opentelemetry.io/otel | v1.11.2 | CVE-2023-47108 | OpenTelemetry-Go Contrib is a collection of third-party packages for OpenTelemetry-Go. Prior to version 0.46.0, the grpc Unary Server Interceptor out of the box adds labels `net.peer.sock.addr` and `net.peer.sock.port` that have unbound cardinality. It leads to the server's potential memory exhaustion when many malicious requests are sent. An attacker can easily flood the peer address and port for requests. Version 0.46.0 contains a fix for this issue. As a workaround to stop being affected, a view removing the attributes can be used. The other possibility is to disable grpc metrics instrumentation by passing `otelgrpc.WithMeterProvider` option with `noop.NewMeterProvider`. | Ažuriranje na verziju 0.46.0 ili noviju kako bi ispravili ovu sigurnosnu ranjivost. Ako trenutno ne možemo ažurirati, razmotriti korišćenje nekog od workaround-ova navedenih u poruci, kao što je korišćenje pogleda koji uklanja sporne atribute ili onemogućavanje grpc metrika pomoću otelgrpc.WithMeterProvider opcije sa noop.NewMeterProvider. |
| golang.org/x/crypto | v0.14.0 | CVE-2022-27191  CVE-2021-43565 | 1.The golang.org/x/crypto/ssh package before 0.0.0-20220314234659-1baeb1ce4c0b for Go allows an attacker to crash a server in certain circumstances involving AddHostKey.  2. The x/crypto/ssh package before 0.0.0-20211202192323-5770296d904e of golang.org/x/crypto allows an attacker to panic an SSH server. | 1.Ažuriranje golang.org/x/crypto/ssh paketa na verziju 0.0.0-20220314234659-1baeb1ce4c0b ili noviju, gde je otklonjen ovaj problem.  2.Ažurirati golang.org/x/crypto/ssh paket na verziju 0.0.0-20211202192323-5770296d904e ili noviju kako bi se otklonila ova ranjivost. |
| casbin/casbin | v1.9.1 |  | The filename parameter of the Context.FileAttachment function is not properly sanitized. A maliciously crafted filename can cause the Content-Disposition header to be sent with an unexpected filename value or otherwise modify the Content-Disposition header. For example, a filename of "setup.bat&quot;;x=.txt" will be sent as a file named "setup.bat". If the FileAttachment function is called with names provided by an untrusted source, this may permit an attacker to cause a file to be served with a name different than provided. Maliciously crafted attachment file name can modify the Content-Disposition header. | Rešenje bi bilo pravilno sanitizovanje naziva datoteke pre nego što se koristi u Content-Disposition zaglavlju. To obuhvata uklanjanje nepoželjnih karaktera ili escapovanje specijalnih karaktera kako bi se sprečila zloupotreba. Ovaj postupak bi trebalo primeniti prilikom obrade naziva datoteke dobijenih od korisnika ili drugih nepouzdanih izvora. |
| /cristalhq/jwt/v4 | v4.0.2 | CVE-2020-22334  CVE-2020-18131 | 1.Cross Site Request Forgery (CSRF) vulnerability in beescms v4 allows attackers to delete the administrator account via crafted request to /admin/admin\_admin.php.  2. Cross Site Request Forgery (CSRF) vulnerability in Bluethrust Clan Scripts v4 allows attackers to escilate privledges to an arbitrary account via a crafted request to /members/console.php?cID=5. | 1.Ažurirati beescms na najnoviju verziju koja ispravlja ovu ranjivost. Takođe, preduzimanje mera zaštite kao što su implementacija CSRF tokena može dodatno poboljšati bezbednost veb aplikacije.  2.Ažuriranje Bluethrust Clan Scripts na najnoviju verziju koja ispravlja ovu ranjivost. Takođe, implementacija dodatnih sigurnosnih mera, poput korišćenja CSRF tokena, može dodatno poboljšati bezbednost veb aplikacije. |
| /gorilla/mux | v1.8.0 | CVE-2017-20146 | Usage of the CORS handler may apply improper CORS headers, allowing the requester to explicitly control the value of the Access-Control-Allow-Origin header, which bypasses the expected behavior of the Same Origin Policy. | Pazljivo konfigurisati CORS zaglavlja tako da ispravno ograniče pristup resursima sa drugih domena u skladu sa očekivanim ponašanjem Same Origin Policy. Postavljanje Access-Control-Allow-Origin zaglavlja na odgovarajuće vrednosti, kao što su dozvoljeni domeni koji imaju pristup resursima, ili upotrebu wildcard (\*) ako je odgovarajuće. Takođe, treba pažljivo proveriti sve resurse koji se dele preko CORS-a kako bi se osiguralo da ne postoji mogućnost da napadač kontroliše vrednost ovog zaglavlja. |
| google/uuid | v1.4.0 | CVE-2021-22571  CVE-2015-5237 | 1.A local attacker could read files from some other users' SA360 reports stored in the /tmp folder during staging process before the files are loaded in BigQuery. We recommend upgrading to version 1.0.3 or above.  2. Protobuf allows remote authenticated attackers to cause a heap-based buffer overflow. | 1.Ažuriranje na verziju 1.0.3 ili noviju.  2. Ažuriranje na noviju verziju biblioteke protobuf koja ispravlja ovu grešku ili primenu zakrpe koja je dostupna od strane razvojnog tima. |
| @angular | v14.1.0 | CVE-2023-26118  CVE-2022-25869 | 1.Versions of the package angular from 1.4.9 are vulnerable to Regular Expression Denial of Service (ReDoS) via the <input type="url"> element due to the usage of an insecure regular expression in the input[url] functionality. Exploiting this vulnerability is possible by a large carefully-crafted input, which can result in catastrophic backtracking.  2.All versions of package angular are vulnerable to Cross-site Scripting (XSS) due to insecure page caching in the Internet Explorer browser, which allows interpolation of <textarea> elements. | 1.Azuriranje verzije paketa Angular na verziju 1.4.10 ili noviju. U ovim novijim verzijama, problem sa regularnim izrazom je ispravljen, smanjujući rizik od ReDoS napada.  2. Da bismo smanjili rizik od ovog napada, preporučuje se ažuriranje Internet Explorer pregledača na najnoviju verziju ili korišćenje alternativnih pregledača koji ne pate od ove ranjivosti. Takođe, možemo koristiti bezbednosne mehanizme kao što su Content Security Policy (CSP) kako bismo ograničili izvršavanje skriptova sa drugih domena. |
| jquery | @3.7.1 | CVE-2007-2379  CVE-2020-23064 | 1.The jQuery framework exchanges data using JavaScript Object Notation (JSON) without an associated protection scheme, which allows remote attackers to obtain the data via a web page that retrieves the data through a URL in the SRC attribute of a SCRIPT element and captures the data using other JavaScript code, aka "JavaScript Hijacking."  2. Cross Site Scripting vulnerability in jQuery 2.2.0 through 3.x before 3.5.0 allows a remote attacker to execute arbitrary code via the <options> element. | 1.Najbolji način zaštite od JavaScript Hijacking-a u jQuery frameworku je korišćenje HTTPS protokola za enkripciju komunikacije između klijenta i servera. Takođe, možemo dodatno osigurati podatke kroz enkripciju ili korišćenje drugih sigurnosnih mehanizama, ali HTTPS je osnovna preporuka za početak.  2. Ažuriranje na najnoviju verziju jQuery (3.5.0 ili novija) kako bi se ispravila ova ranjivost. |
| sirupsen/logrus | V1.9.3 | CVE-2024-24760  CVE-2024-24757 | 1.mailcow is a dockerized email package, with multiple containers linked in one bridged network. A security vulnerability has been identified in mailcow affecting versions < 2024-01c. This vulnerability potentially allows attackers on the same subnet to connect to exposed ports of a Docker container, even when the port is bound to 127.0.0.1. The vulnerability has been addressed by implementing additional iptables/nftables rules. These rules drop packets for Docker containers on ports 3306, 6379, 8983, and 12345, where the input interface is not `br-mailcow` and the output interface is `br-mailcow`.  2. open-irs is an issue response robot that reponds to issues in the installed repository. The `.env` file was accidentally uploaded when working with git actions. This problem is fixed in 1.0.1. Discontinuing all sensitive keys and turning into secrets. | 1.Resena je implementiranjem dodatnih pravila iptables/nftables.  2. Ažurirati verziju softvera na 1.0.1 i prestati koristiti osetljive ključeve, umesto toga ih treba čuvati kao tajne. |
| natefinch/lumberjack | v2.2.1 | CVE-2015-5619 | Logstash 1.4.x before 1.4.5 and 1.5.x before 1.5.4 with Lumberjack output or the Logstash forwarder does not validate SSL/TLS certificates from the Logstash server, which might allow attackers to obtain sensitive information via a man-in-the-middle attack. | Ažuriranje Logstash-a na verziju 1.4.5 ili noviju za verziju 1.4.x, i verziju 1.5.4 ili noviju za verziju 1.5.x. Ovo će omogućiti pravilnu validaciju SSL/TLS sertifikata i smanjiti rizik od napada "man-in-the-middle". |