

BoringSSL-GRPC 0.0.7:

* Google gRPC before 2017-03-29 has an out-of-bounds write caused by a heap-based use-after-free related to the `grpc_call_destroy` function in `core/lib/surface/call.c`. -

Google gRPC before 2017-03-29 has an out-of-bounds write caused by a heap-based use-after-free related to the `grpc_call_destroy` function in `core/lib/surface/call.c`.

* Google gRPC before 2017-02-22 has an out-of-bounds write related to the `gpr_free` function in `core/lib/support/alloc.c`. -

Google gRPC before 2017-02-22 has an out-of-bounds write related to the `gpr_free` function in `core/lib/support/alloc.c`.

* Google gRPC before 2017-04-05 has an out-of-bounds write caused by a heap-based buffer overflow related to `core/lib/iomgr/error.c`. -

Google gRPC before 2017-04-05 has an out-of-bounds write caused by a heap-based buffer overflow related to `core/lib/iomgr/error.c`.

* Google gRPC before 2017-02-22 has an out-of-bounds write caused by a heap-based buffer overflow related to the `parse_unix` function in `core/ext/client_channel/parse_address.c`. -

Google gRPC before 2017-02-22 has an out-of-bounds write caused by a heap-based buffer overflow related to the `parse_unix` function in `core/ext/client_channel/parse_address.c`.

* The package `grpc` before 1.24.4; the package `@grpc/grpc-js` before 1.1.8 are vulnerable to Prototype Pollution via `loadPackageDefinition`. -

The package `grpc` before 1.24.4; the package `@grpc/grpc-js` before 1.1.8 are vulnerable to Prototype Pollution via `loadPackageDefinition`.

File to review: `.\ios`

`Podfile.lock`

GoogleUtilities/AppDelegateSwizzler 7.2.0:

* Multiple buffer overflows in `DeleGate` before 8.11.1 may allow attackers to cause a denial of service or execute arbitrary code, possibly due to "overflows on arrays." -

Multiple buffer overflows in `DeleGate` before 8.11.1 may allow attackers to cause a denial of service or execute arbitrary code, possibly due to "overflows on arrays."

* The DNS implementation in `DeleGate` 8.10.2 and earlier allows remote attackers to cause a denial of service via a compressed DNS packet with a label length byte with an incorrect offset, which could trigger an infinite loop. -

The DNS implementation in `DeleGate` 8.10.2 and earlier allows remote attackers to cause a denial of service via a compressed DNS packet with a label length byte with an incorrect offset, which could trigger an infinite loop.

File to review: `.\ios`

`Podfile.lock`

abseil/base/throw_delegate 0.20200225.0:

* Multiple buffer overflows in DeleGate before 8.11.1 may allow attackers to cause a denial of service or execute arbitrary code, possibly due to "overflows on arrays." -

Multiple buffer overflows in DeleGate before 8.11.1 may allow attackers to cause a denial of service or execute arbitrary code, possibly due to "overflows on arrays."

* The DNS implementation in DeleGate 8.10.2 and earlier allows remote attackers to cause a denial of service via a compressed DNS packet with a label length byte with an incorrect offset, which could trigger an infinite loop. -

The DNS implementation in DeleGate 8.10.2 and earlier allows remote attackers to cause a denial of service via a compressed DNS packet with a label length byte with an incorrect offset, which could trigger an infinite loop.

* Delegate proxy 5.9.3 and earlier creates files and directories in the DGROOT with world-writable permissions. -

Delegate proxy 5.9.3 and earlier creates files and directories in the DGROOT with world-writable permissions.

File to review: .\ios
Podfile.lock