The REST API is now versioned. For more information, see "About API versioning."

Global security advisories

Use the REST API to view global security advisories.

List global security advisories

Works with GitHub Apps

Lists all global security advisories that match the specified parameters. If no other parameters are defined, the request will return only GitHub-reviewed advisories that are not malware.

By default, all responses will exclude advisories for malware, because malware are not standard vulnerabilities. To list advisories for malware, you must include the `type` parameter in your request, with the value `malware`. For more information about the different types of security advisories, see "About the GitHub Advisory database."

Parameters for "List global security advisories"

Headers

`accept` string

Setting to `application/vnd.github+json` is recommended.

Query parameters

`ghsa_id` string

If specified, only advisories with this GHSA (GitHub Security Advisory) identifier will be returned.

`type` string

If specified, only advisories of this type will be returned. By default, a request with no other parameters defined will only return reviewed advisories that are not malware.

Default: `reviewed`
Can be one of: `reviewed`, `malware`, `unreviewed`

`cve_id` string

If specified, only advisories with this CVE (Common Vulnerabilities and Exposures) identifier will be returned.

`ecosystem` string

If specified, only advisories for these ecosystems will be returned.

Can be one of: `actions`, `composer`, `erlang`, `go`, `maven`, `npm`, `nuget`, `other`, `pip`, `pub`, `rubygems`, `rust`

`severity` string

If specified, only advisories with these severities will be returned.

Can be one of: `unknown`, `low`, `medium`, `high`, `critical`

Can be one of: `unknown`, `low`, `medium`, `high`, `critical`

`cwes`

If specified, only advisories with these Common Weakness Enumerations (CWEs) will be returned.
Example: `cwes=79,284,22` or `cwes[]=79&cwes[]=284&cwes[]=22`

`is_withdrawn` boolean

Whether to only return advisories that have been withdrawn.

`affects`

If specified, only return advisories that affect any of `package` or `package@version`. A maximum of 1000 packages can be specified. If the query parameter causes the URL to exceed the maximum URL length supported by your client, you must specify fewer packages.
Example: `affects=package1,package2@1.0.0,package3@^2.0.0` or `affects[]=package1&affects[]=package2@1.0.0`

`published` string

If specified, only return advisories that were published on a date or date range.
For more information on the syntax of the date range, see "Understanding the search syntax."

`updated` string

If specified, only return advisories that were updated on a date or date range.
For more information on the syntax of the date range, see "Understanding the search syntax."

`modified` string

If specified, only show advisories that were updated or published on a date or date range.
For more information on the syntax of the date range, see "Understanding the search syntax."

`before` string

A cursor, as given in the Link header. If specified, the query only searches for results before this cursor.

`after` string

A cursor, as given in the Link header. If specified, the query only searches for results after this cursor.

`direction` string

The direction to sort the results by.

Default: `desc`
Can be one of: `asc`, `desc`

`per_page` integer

The number of results per page (max 100).

Default: `30`

`sort` string

The property to sort the results by.

Default: `published`
Can be one of: `updated`, `published`

HTTP response status codes for "List global security advisories"

Status code	Description
`200`	OK
`422`	Validation failed, or the endpoint has been spammed.

429	Too many requests

Code samples for "List global security advisories"

GET /advisories

cURL | JavaScript | GitHub CLI

```
curl -L \ -H "Accept: application/vnd.github+json" \ -H "Authorization: Bearer <YOUR-TOKEN>" \ -H "X-GitHub-Api-Version: 2022-11-28" \ https://api.github.com/advisories
```

Response

Example response | Response schema

```
Status: 200
```


```
[ { "id": 1, "ghsa_id": "GHSA-abcd-1234-efgh", "cve_id": "CVE-2050-00000", "url": "https://api.github.com/advisories/GHSA-abcd-1234-efgh", "html_url": "https://github.com/advisories/GHSA-abcd-1234-efgh", "repository_advisory_url": "https://api.github.com/repos/project/a-package/security-advisories/GHSA-abcd-1234-efgh", "summary": "Heartbleed security advisory", "description": "This bug allows an attacker to read portions of the affected server’s memory, potentially disclosing sensitive information.", "type": "reviewed", "severity": "high", "source_code_location": "https://github.com/project/a-package", "identifiers": [ { "type": "GHSA", "value": "GHSA-abcd-1234-efgh" }, { "type": "CVE", "value": "CVE-2050-00000" } ], "references":
```


Get a global security advisory

Works with GitHub Apps

Gets a global security advisory using its GitHub Security Advisory (GHSA) identifier.

Parameters for "Get a global security advisory"

Headers

accept string

Setting to `application/vnd.github+json` is recommended.

Path parameters

ghsa_id string Required

The GHSA (GitHub Security Advisory) identifier of the advisory.

HTTP response status codes for "Get a global security advisory"

Status code	Description
200	OK
404	Resource not found

Code samples for "Get a global security advisory"

GET /advisories/{ghsa_id}

cURL | JavaScript | GitHub CLI

```
curl -L \ -H "Accept: application/vnd.github+json" \ -H "Authorization: Bearer <YOUR-TOKEN>" \ -H "X-GitHub-Api-Version: 2022-11-28" \ https://api.github.com/advisories/GHSA_ID
```

Response

Example response | Response schema

Status: 200


```
{ "ghsa_id": "GHSA-abcd-1234-efgh", "cve_id": "CVE-2050-00000", "url": "https://api.github.com/advisories/GHSA-abcd-1234-efgh", "html_url": "https://github.com/advisories/GHSA-abcd-1234-efgh", "repository_advisory_url": "https://api.github.com/repos/project/a-package/security-advisories/GHSA-abcd-1234-efgh", "summary": "A short summary of the advisory.", "description": "A detailed description of what the advisory entails.", "type": "reviewed", "severity": "high", "source_code_location": "https://github.com/project/a-package", "identifiers": [ { "type": "GHSA", "value": "GHSA-abcd-1234-efgh" }, { "type": "CVE", "value": "CVE-2050-00000" } ], "references": [ "https://nvd.nist.gov/vuln/detail/CVE-2050-00000" ],
```