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

Repository security advisories

Use the REST API to view and manage repository security advisories.

List repository security advisories for an organization

✓ Works with GitHub Apps

Lists repository security advisories for an organization.

To use this endpoint, you must be an owner or security manager for the organization, and you must use an access token with the `repo` scope or `repository_advisories:write` permission.

Parameters for "List repository security advisories for an organization"

Headers

`accept` string

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

Path parameters

`org` string Required

The organization name. The name is not case sensitive.

Query parameters

`direction` string

The direction to sort the results by.

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

`sort` string

The property to sort the results by.

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

`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.

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

per_page integer

The number of advisories to return per page.

Default: `30`

state string

Filter by the state of the repository advisories. Only advisories of this state will be returned.

Can be one of: `triage`, `draft`, `published`, `closed`

HTTP response status codes for "List repository security advisories for an organization"

Status code	Description
`200`	OK
`400`	Bad Request
`404`	Resource not found

Code samples for "List repository security advisories for an organization"

GET /orgs/{org}/security-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/orgs/ORG/security-advisories
```

Response

Example response Response schema

Status: 200

```
[ { "ghsa_id": "GHSA-abcd-1234-efgh", "cve_id": "CVE-2050-00000", "url": "https://api.github.com/repos/repo/a-package/security-advisories/GHSA-abcd-1234-efgh", "html_url": "https://github.com/repo/a-package/security/advisories/GHSA-abcd-1234-efgh", "summary": "A short summary of the advisory.", "description": "A detailed description of what the advisory entails.", "severity": "critical", "author": { "login": "octocat", "id": 1, "node_id": "MDQ6VXNlcjE=", "avatar_url": "https://github.com/images/error/octocat_happy.gif", "gravatar_id": "", "url": "https://api.github.com/users/octocat", "html_url": "https://github.com/octocat", "followers_url": "https://api.github.com/users/octocat/followers", "following_url":
```

List repository security advisories

✓ Works with GitHub Apps

Lists security advisories in a repository. You must authenticate using an access token with the `repo` scope or `repository_advisories:read` permission in order to get published security advisories in a private repository, or any unpublished security advisories that you have access to.

You can access unpublished security advisories from a repository if you are a security manager or administrator of that repository, or if you are a collaborator on any security advisory.

Parameters for "List repository security advisories"

Headers

`accept` string

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

Path parameters

`owner` string Required

The account owner of the repository. The name is not case sensitive.

`repo` string Required

The name of the repository without the `.git` extension. The name is not case sensitive.

Query parameters

`direction` string

The direction to sort the results by.

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

`sort` string

The property to sort the results by.

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

`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.

`per_page` integer

Number of advisories to return per page.

Default: `30`

`state` string

Filter by state of the repository advisories. Only advisories of this state will be returned.

Can be one of: `triage`, `draft`, `published`, `closed`

HTTP response status codes for "List repository security advisories"

Status code	Description
`200`	OK
`400`	Bad Request
`404`	Resource not found

Code samples for "List repository security advisories"

GET /repos/{owner}/{repo}/security-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/repos/OWNER/REPO/security-advisories
```

Response

Example response Response schema

Status: 200

```
[ { "ghsa_id": "GHSA-abcd-1234-efgh", "cve_id": "CVE-2050-00000", "url": "https://api.github.com/repos/repo/a-package/security-
advisories/GHSA-abcd-1234-efgh", "html_url": "https://github.com/repo/a-package/security/advisories/GHSA-abcd-1234-efgh",
"summary": "A short summary of the advisory.", "description": "A detailed description of what the advisory entails.", "severity":
"critical", "author": { "login": "octocat", "id": 1, "node_id": "MDQ6VXNlcjE=", "avatar_url":
"https://github.com/images/error/octocat_happy.gif", "gravatar_id": "", "url": "https://api.github.com/users/octocat", "html_url":
"https://github.com/octocat", "followers_url": "https://api.github.com/users/octocat/followers", "following_url":
```

Create a repository security advisory

Works with GitHub Apps

Creates a new repository security advisory. You must authenticate using an access token with the `repo` scope or `repository_advisories:write` permission to use this endpoint.

In order to create a draft repository security advisory, you must be a security manager or administrator of that repository.

Parameters for "Create a repository security advisory"

Headers

`accept` string

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

Path parameters

`owner` string Required

The account owner of the repository. The name is not case sensitive.

`repo` string Required

The name of the repository without the `.git` extension. The name is not case sensitive.

Body parameters

`summary` string Required

`summary` string Required

A short summary of the advisory.

`description` string Required

A detailed description of what the advisory impacts.

`cve_id` string or null

The Common Vulnerabilities and Exposures (CVE) ID.

`vulnerabilities` array of objects Required

A product affected by the vulnerability detailed in a repository security advisory.

▶ Properties of `vulnerabilities`

`cwe_ids` array of strings or null

A list of Common Weakness Enumeration (CWE) IDs.

`credits` array of objects or null

A list of users receiving credit for their participation in the security advisory.

▶ Properties of `credits`

`severity` string or null

The severity of the advisory. You must choose between setting this field or `cvss_vector_string`.

Can be one of: `critical`, `high`, `medium`, `low`, *`null`*

`cvss_vector_string` string or null

The CVSS vector that calculates the severity of the advisory. You must choose between setting this field or `severity`.

HTTP response status codes for "Create a repository security advisory"

Status code	Description
`201`	Created
`403`	Forbidden
`404`	Resource not found
`422`	Validation failed, or the endpoint has been spammed.

Code samples for "Create a repository security advisory"

POST /repos/{owner}/{repo}/security-advisories

cURL JavaScript

```
curl -L \ -X POST \ -H "Accept: application/vnd.github+json" \ -H "Authorization: Bearer <YOUR-TOKEN>" \ -H "X-GitHub-Api-Version:
2022-11-28" \ https://api.github.com/repos/OWNER/REPO/security-advisories \ -d '{"summary":"A new important
advisory","description":"A more in-depth description of what the problem is.","severity":"high","cve_id":null,"vulnerabilities":
[{"package":{"name":"a-package","ecosystem":"npm"},"vulnerable_version_range":"<
1.0.0","patched_versions":"1.0.0","vulnerable_functions":["important_function"]}],"cwe_ids":["CWE-1101","CWE-20"],"credits":
[{"login":"monalisa","type":"reporter"},{"login":"octocat","type":"analyst"}]}'
```

Response

Example response Response schema

Status: 201

```
{ "ghsa_id": "GHSA-abcd-1234-efgh", "cve_id": "CVE-2050-00000", "url": "https://api.github.com/repos/repo/a-package/security-advisories/GHSA-abcd-1234-efgh", "html_url": "https://github.com/repo/a-package/security/advisories/GHSA-abcd-1234-efgh", "summary": "A short summary of the advisory.", "description": "A detailed description of what the advisory entails.", "severity": "critical", "author": { "login": "octocat", "id": 1, "node_id": "MDQ6VXNlcjE=", "avatar_url": "https://github.com/images/error/octocat_happy.gif", "gravatar_id": "", "url": "https://api.github.com/users/octocat", "html_url": "https://github.com/octocat", "followers_url": "https://api.github.com/users/octocat/followers", "following_url":
```

Privately report a security vulnerability

✓ Works with GitHub Apps

Report a security vulnerability to the maintainers of the repository. See "Privately reporting a security vulnerability" for more information about private vulnerability reporting.

Parameters for "Privately report a security vulnerability"

Headers

`accept` string

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

Path parameters

`owner` string Required

The account owner of the repository. The name is not case sensitive.

`repo` string Required

The name of the repository without the `.git` extension. The name is not case sensitive.

Body parameters

`summary` string Required

A short summary of the advisory.

`description` string Required

A detailed description of what the advisory impacts.

`vulnerabilities` array of objects or null

An array of products affected by the vulnerability detailed in a repository security advisory.

▶ Properties of `vulnerabilities`

`cwe_ids` array of strings or null

A list of Common Weakness Enumeration (CWE) IDs.

`severity` string or null

The severity of the advisory. You must choose between setting this field or `cvss_vector_string`.

Can be one of: `critical`, `high`, `medium`, `low`, *`null`*

`cvss_vector_string` string or null

The CVSS vector that calculates the severity of the advisory. You must choose between setting this field or `severity`.

HTTP response status codes for "Privately report a security vulnerability"

Status code	Description
`201`	Created
`403`	Forbidden
`404`	Resource not found
`422`	Validation failed, or the endpoint has been spammed.

Code samples for "Privately report a security vulnerability"

POST `/repos/{owner}/{repo}/security-advisories/reports`

cURL JavaScript GitHub CLI

```
 curl -L \ -X POST \ -H "Accept: application/vnd.github+json" \ -H "Authorization: Bearer <YOUR-TOKEN>" \ -H "X-GitHub-Api-Version:
2022-11-28" \ https://api.github.com/repos/OWNER/REPO/security-advisories/reports \ -d '{"summary":"A newly discovered
vulnerability","description":"A more in-depth description of what the problem is.","severity":"high","vulnerabilities":[{"package":
{"name":"a-package","ecosystem":"npm"},"vulnerable_version_range":"< 1.0.0","patched_versions":"1.0.0","vulnerable_functions":
["important_function"]}],"cwe_ids":["CWE-123"]}'
```

Response

Example response Response schema

```
Status: 201
```

```
 { "ghsa_id": "GHSA-abcd-1234-efgh", "cve_id": "CVE-2050-00000", "url": "https://api.github.com/repos/repo/a-package/security-
advisories/GHSA-abcd-1234-efgh", "html_url": "https://github.com/repo/a-package/security/advisories/GHSA-abcd-1234-efgh",
"summary": "A newly discovered vulnerability", "description": "A more in-depth description of what the problem is.", "severity":
"high", "author": { "login": "octocat", "id": 1, "node_id": "MDQ6VXNlcjE=", "avatar_url":
"https://github.com/images/error/octocat_happy.gif", "gravatar_id": "", "url": "https://api.github.com/users/octocat", "html_url":
"https://github.com/octocat", "followers_url": "https://api.github.com/users/octocat/followers", "following_url":
```

Get a repository security advisory

✓ Works with GitHub Apps

Get a repository security advisory using its GitHub Security Advisory (GHSA) identifier. You can access any published security advisory on a public repository. You must authenticate using an access token with the `repo` scope or `repository_advisories:read` permission in order to get a published security advisory in a private repository, or any unpublished security advisory that you have access to.

You can access an unpublished security advisory from a repository if you are a security manager or administrator of that repository, or if you are a collaborator on the security advisory.

Parameters for "Get a repository security advisory"

Headers

`accept` string

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

Path parameters

`owner` string Required

The account owner of the repository. The name is not case sensitive.

`repo` string Required

The name of the repository without the `.git` extension. The name is not case sensitive.

`ghsa_id` string Required

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

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

Status code	Description
`200`	OK
`403`	Forbidden
`404`	Resource not found

Code samples for "Get a repository security advisory"

GET `/repos/{owner}/{repo}/security-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/repos/OWNER/REPO/security-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/repos/repo/a-package/security-advisories/GHSA-abcd-1234-efgh", "html_url": "https://github.com/repo/a-package/security/advisories/GHSA-abcd-1234-efgh", "summary": "A short summary of the advisory.", "description": "A detailed description of what the advisory entails.", "severity": "critical", "author": { "login": "octocat", "id": 1, "node_id": "MDQ6VXNlcjE=", "avatar_url": "https://github.com/images/error/octocat_happy.gif", "gravatar_id": "", "url": "https://api.github.com/users/octocat", "html_url": "https://github.com/octocat", "followers_url": "https://api.github.com/users/octocat/followers", "following_url":

Update a repository security advisory

✓ Works with GitHub Apps

Update a repository security advisory using its GitHub Security Advisory (GHSA) identifier. You must authenticate using an access token with the `repo` scope or `repository_advisories:write` permission to use this endpoint.

In order to update any security advisory, you must be a security manager or administrator of that repository, or a collaborator on the repository security advisory.

Parameters for "Update a repository security advisory"

Headers

`accept` string

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

Path parameters

`owner` string Required

The account owner of the repository. The name is not case sensitive.

`repo` string Required

The name of the repository without the `.git` extension. The name is not case sensitive.

`ghsa_id` string Required

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

Body parameters

`summary` string

A short summary of the advisory.

`description` string

A detailed description of what the advisory impacts.

`cve_id` string or null

The Common Vulnerabilities and Exposures (CVE) ID.

`vulnerabilities` array of objects

A product affected by the vulnerability detailed in a repository security advisory.

▶ Properties of `vulnerabilities`

`cwe_ids` array of strings or null

A list of Common Weakness Enumeration (CWE) IDs.

`credits` array of objects or null

A list of users receiving credit for their participation in the security advisory.

▶ Properties of `credits`

`severity` string or null

The severity of the advisory. You must choose between setting this field or `cvss_vector_string`.

Can be one of: `critical`, `high`, `medium`, `low`, *`null`*

`cvss_vector_string` string or null

The CVSS vector that calculates the severity of the advisory. You must choose between setting this field or `severity`.

`state` string

The state of the advisory.

Can be one of: `published`, `closed`, `draft`

`collaborating_users` array of strings or null

A list of usernames who have been granted write access to the advisory.

`collaborating_teams` array of strings or null

A list of team slugs which have been granted write access to the advisory.

HTTP response status codes for "Update a repository security advisory"

Status code	Description
`200`	OK
`403`	Forbidden
`404`	Resource not found
`422`	Validation failed, or the endpoint has been spammed.

Code samples for "Update a repository security advisory"

Updating the severity and state.

PATCH `/repos/{owner}/{repo}/security-advisories/{ghsa_id}`

cURL JavaScript GitHub CLI

```
curl -L \ -X PATCH \ -H "Accept: application/vnd.github+json" \ -H "Authorization: Bearer <YOUR-TOKEN>" \ -H "X-GitHub-Api-Version:
2022-11-28" \ https://api.github.com/repos/OWNER/REPO/security-advisories/GHSA_ID \ -d '{"severity":"critical","state":"published"}'
```

Response

Example response Response schema

```
Status: 200
```

{ "ghsa_id": "GHSA-abcd-1234-efgh", "cve_id": "CVE-2050-00000", "url": "https://api.github.com/repos/repo/a-package/security-

```
advisories/GHSA-abcd-1234-efgh", "html_url": "https://github.com/repo/a-package/security/advisories/GHSA-abcd-1234-efgh",
"summary": "A short summary of the advisory.", "description": "A detailed description of what the advisory entails.", "severity":
"critical", "author": { "login": "octocat", "id": 1, "node_id": "MDQ6VXNlcjE=", "avatar_url":
"https://github.com/images/error/octocat_happy.gif", "gravatar_id": "", "url": "https://api.github.com/users/octocat", "html_url":
"https://github.com/octocat", "followers_url": "https://api.github.com/users/octocat/followers", "following_url":
```

Request a CVE for a repository security advisory

Works with GitHub Apps

If you want a CVE identification number for the security vulnerability in your project, and don't already have one, you can request a CVE identification number from GitHub. For more information see "Requesting a CVE identification number."

You may request a CVE for public repositories, but cannot do so for private repositories.

You must authenticate using an access token with the `repo` scope or `repository_advisories:write` permission to use this endpoint.

In order to request a CVE for a repository security advisory, you must be a security manager or administrator of that repository.

Parameters for "Request a CVE for a repository security advisory"

Headers

`accept` string

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

Path parameters

`owner` string Required

The account owner of the repository. The name is not case sensitive.

`repo` string Required

The name of the repository without the `.git` extension. The name is not case sensitive.

`ghsa_id` string Required

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

HTTP response status codes for "Request a CVE for a repository security advisory"

Status code	Description
`202`	Accepted
`400`	Bad Request
`403`	Forbidden
`404`	Resource not found

422	Validation failed, or the endpoint has been spammed.

Code samples for "Request a CVE for a repository security advisory"

POST /repos/{owner}/{repo}/security-advisories/{ghsa_id}/cve

cURL JavaScript GitHub CLI

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

Accepted

Example response Response schema

```
Status: 202
```