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

# Dependabot alerts

Use the REST API to interact with Dependabot alerts for a repository.

**Note**: The ability to use the REST API to manage Dependabot alerts is currently in public beta and subject to change.

## About Dependabot alerts

You can view Dependabot alerts for a repository and update individual alerts with the REST API. For more information, see "About Dependabot alerts."

## List Dependabot alerts for an enterprise

Lists Dependabot alerts for repositories that are owned by the specified enterprise. To use this endpoint, you must be a member of the enterprise, and you must use an access token with the `repo` scope or `security_events` scope. Alerts are only returned for organizations in the enterprise for which you are an organization owner or a security manager. For more information about security managers, see "Managing security managers in your organization."

### Parameters for "List Dependabot alerts for an enterprise"

#### Headers

**`accept`** string

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

#### Path parameters

**`enterprise`** string Required

The slug version of the enterprise name. You can also substitute this value with the enterprise id.

#### Query parameters

**`state`** string

A comma-separated list of states. If specified, only alerts with these states will be returned.
Can be: `auto_dismissed`, `dismissed`, `fixed`, `open`

**`severity`** string

A comma-separated list of severities. If specified, only alerts with these severities will be returned.
Can be: `low`, `medium`, `high`, `critical`

**`ecosystem`** string

**ecosystem** string

A comma-separated list of ecosystems. If specified, only alerts for these ecosystems will be returned.
Can be: `composer`, `go`, `maven`, `npm`, `nuget`, `pip`, `pub`, `rubygems`, `rust`

---

**package** string

A comma-separated list of package names. If specified, only alerts for these packages will be returned.

---

**scope** string

The scope of the vulnerable dependency. If specified, only alerts with this scope will be returned.

Can be one of: `development`, `runtime`

---

**sort** string

The property by which to sort the results. `created` means when the alert was created. `updated` means when the alert's state last changed.

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

---

**direction** string

The direction to sort the results by.

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

---

**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.

---

**first** integer

**Deprecated**. The number of results per page (max 100), starting from the first matching result. This parameter must not be used in combination with `last`. Instead, use `per_page` in combination with `after` to fetch the first page of results.

Default: `30`

---

**last** integer

**Deprecated**. The number of results per page (max 100), starting from the last matching result. This parameter must not be used in combination with `first`. Instead, use `per_page` in combination with `before` to fetch the last page of results.

---

**per_page** integer

The number of results per page (max 100).

Default: `30`

### HTTP response status codes for "List Dependabot alerts for an enterprise"

| Status code | Description |
| --- | --- |
| `200` | OK |
| `304` | Not modified |
| `403` | Forbidden |
| `404` | Resource not found |
| `422` | Validation failed, or the endpoint has been spammed. |

### Code samples for "List Dependabot alerts for an enterprise"

GET /enterprises/{enterprise}/dependabot/alerts

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" \ http(s)://HOSTNAME/api/v3/enterprises/ENTERPRISE/dependabot/alerts
```

### Response

Example response | Response schema

Status: 200


```
[ { "number": 2, "state": "dismissed", "dependency": { "package": { "ecosystem": "pip", "name": "django" }, "manifest_path": "path/to/requirements.txt", "scope": "runtime" }, "security_advisory": { "ghsa_id": "GHSA-rf4j-j272-fj86", "cve_id": "CVE-2018-6188", "summary": "Django allows remote attackers to obtain potentially sensitive information by leveraging data exposure from the confirm_login_allowed() method, as demonstrated by discovering whether a user account is inactive", "description": "django.contrib.auth.forms.AuthenticationForm in Django 2.0 before 2.0.2, and 1.11.8 and 1.11.9, allows remote attackers to obtain potentially sensitive information by leveraging data exposure from the confirm_login_allowed() method, as demonstrated by
```


## List Dependabot alerts for an organization

Works with GitHub Apps

Lists Dependabot alerts 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 `security_events` scope.

For public repositories, you may instead use the `public_repo` scope.

GitHub Apps must have **Dependabot alerts** read permission to use this endpoint.

### Parameters for "List Dependabot alerts 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

**state** string

A comma-separated list of states. If specified, only alerts with these states will be returned.
Can be: `auto_dismissed`, `dismissed`, `fixed`, `open`

---

**`severity`** string

A comma-separated list of severities. If specified, only alerts with these severities will be returned.
Can be: `low`, `medium`, `high`, `critical`

---

**`ecosystem`** string

A comma-separated list of ecosystems. If specified, only alerts for these ecosystems will be returned.
Can be: `composer`, `go`, `maven`, `npm`, `nuget`, `pip`, `pub`, `rubygems`, `rust`

---

**`package`** string

A comma-separated list of package names. If specified, only alerts for these packages will be returned.

---

**`scope`** string

The scope of the vulnerable dependency. If specified, only alerts with this scope will be returned.

Can be one of: `development`, `runtime`

---

**`sort`** string

The property by which to sort the results. `created` means when the alert was created. `updated` means when the alert's state last changed.

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

---

**`direction`** string

The direction to sort the results by.

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

---

**`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.

---

**`first`** integer

**Deprecated**. The number of results per page (max 100), starting from the first matching result. This parameter must not be used in combination with `last`. Instead, use `per_page` in combination with `after` to fetch the first page of results.

Default: `30`

---

**`last`** integer

**Deprecated**. The number of results per page (max 100), starting from the last matching result. This parameter must not be used in combination with `first`. Instead, use `per_page` in combination with `before` to fetch the last page of results.

---

**`per_page`** integer

The number of results per page (max 100).

Default: `30`

### HTTP response status codes for "List Dependabot alerts for an organization"

| Status code | Description |
| --- | --- |
| `200` | OK |

| | |
|---|---|
| `304` | Not modified |
| `400` | Bad Request |
| `403` | Forbidden |
| `404` | Resource not found |
| `422` | Validation failed, or the endpoint has been spammed. |

### Code samples for "List Dependabot alerts for an organization"

`GET` `/orgs/{org}/dependabot/alerts`

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" \ http(s)://HOSTNAME/api/v3/orgs/ORG/dependabot/alerts
```

### Response

Example response | Response schema

Status: 200


```
[ { "number": 2, "state": "dismissed", "dependency": { "package": { "ecosystem": "pip", "name": "django" }, "manifest_path": "path/to/requirements.txt", "scope": "runtime" }, "security_advisory": { "ghsa_id": "GHSA-rf4j-j272-fj86", "cve_id": "CVE-2018-6188", "summary": "Django allows remote attackers to obtain potentially sensitive information by leveraging data exposure from the confirm_login_allowed() method, as demonstrated by discovering whether a user account is inactive", "description": "django.contrib.auth.forms.AuthenticationForm in Django 2.0 before 2.0.2, and 1.11.8 and 1.11.9, allows remote attackers to obtain potentially sensitive information by leveraging data exposure from the confirm_login_allowed() method, as demonstrated by
```


## List Dependabot alerts for a repository

Works with GitHub Apps

You must use an access token with the `security_events` scope to use this endpoint with private repositories. You can also use tokens with the `public_repo` scope for public repositories only. GitHub Apps must have **Dependabot alerts** read permission to use this endpoint.

### Parameters for "List Dependabot alerts for a repository"

#### 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

---

**`state`** string

A comma-separated list of states. If specified, only alerts with these states will be returned.
Can be: `auto_dismissed`, `dismissed`, `fixed`, `open`

---

**`severity`** string

A comma-separated list of severities. If specified, only alerts with these severities will be returned.
Can be: `low`, `medium`, `high`, `critical`

---

**`ecosystem`** string

A comma-separated list of ecosystems. If specified, only alerts for these ecosystems will be returned.
Can be: `composer`, `go`, `maven`, `npm`, `nuget`, `pip`, `pub`, `rubygems`, `rust`

---

**`package`** string

A comma-separated list of package names. If specified, only alerts for these packages will be returned.

---

**`manifest`** string

A comma-separated list of full manifest paths. If specified, only alerts for these manifests will be returned.

---

**`scope`** string

The scope of the vulnerable dependency. If specified, only alerts with this scope will be returned.

Can be one of: `development`, `runtime`

---

**`sort`** string

The property by which to sort the results. `created` means when the alert was created. `updated` means when the alert's state last changed.

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

---

**`direction`** string

The direction to sort the results by.

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

---

**`page`** integer

**Deprecated**. Page number of the results to fetch. Use cursor-based pagination with `before` or `after` instead.

Default: `1`

---

**`per_page`** integer

The number of results per page (max 100).

Default: `30`

---

**`before`** string

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

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.

**`first`** integer

**Deprecated**. The number of results per page (max 100), starting from the first matching result. This parameter must not be used in combination with `last`. Instead, use `per_page` in combination with `after` to fetch the first page of results.

Default: `30`

**`last`** integer

**Deprecated**. The number of results per page (max 100), starting from the last matching result. This parameter must not be used in combination with `first`. Instead, use `per_page` in combination with `before` to fetch the last page of results.

### HTTP response status codes for "List Dependabot alerts for a repository"

| Status code | Description |
| --- | --- |
| `200` | OK |
| `304` | Not modified |
| `400` | Bad Request |
| `403` | Forbidden |
| `404` | Resource not found |
| `422` | Validation failed, or the endpoint has been spammed. |

### Code samples for "List Dependabot alerts for a repository"

`GET` `/repos/{owner}/{repo}/dependabot/alerts`

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" \ http(s)://HOSTNAME/api/v3/repos/OWNER/REPO/dependabot/alerts
```

### Response

Example response | Response schema

```
Status: 200
```


```
[ { "number": 2, "state": "dismissed", "dependency": { "package": { "ecosystem": "pip", "name": "django" }, "manifest_path": "path/to/requirements.txt", "scope": "runtime" }, "security_advisory": { "ghsa_id": "GHSA-rf4j-j272-fj86", "cve_id": "CVE-2018-6188", "summary": "Django allows remote attackers to obtain potentially sensitive information by leveraging data exposure from the confirm_login_allowed() method, as demonstrated by discovering whether a user account is inactive", "description": "django.contrib.auth.forms.AuthenticationForm in Django 2.0 before 2.0.2, and 1.11.8 and 1.11.9, allows remote attackers to obtain potentially sensitive information by leveraging data exposure from the confirm_login_allowed() method, as demonstrated by
```

# Get a Dependabot alert

Works with GitHub Apps

You must use an access token with the `security_events` scope to use this endpoint with private repositories. You can also use tokens with the `public_repo` scope for public repositories only. GitHub Apps must have **Dependabot alerts** read permission to use this endpoint.

### Parameters for "Get a Dependabot alert"

#### 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.

**`alert_number`** integer Required

The number that identifies a Dependabot alert in its repository. You can find this at the end of the URL for a Dependabot alert within GitHub, or in `number` fields in the response from the `GET /repos/{owner}/{repo}/dependabot/alerts` operation.

### HTTP response status codes for "Get a Dependabot alert"

| Status code | Description |
|---|---|
| `200` | OK |
| `304` | Not modified |
| `403` | Forbidden |
| `404` | Resource not found |

### Code samples for "Get a Dependabot alert"

`GET` `/repos/{owner}/{repo}/dependabot/alerts/{alert_number}`

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" \ http(s)://HOSTNAME/api/v3/repos/OWNER/REPO/dependabot/alerts/ALERT_NUMBER
```

#### Response

Example response | Response schema

```
Status: 200
```


```
{ "number": 1, "state": "open", "dependency": { "package": { "ecosystem": "pip", "name": "ansible" }, "manifest_path": "path/to/requirements.txt", "scope": "runtime" }, "security_advisory": { "ghsa_id": "GHSA-8f4m-hccc-8qph", "cve_id": "CVE-2021-20191", "summary": "Insertion of Sensitive Information into Log File in ansible", "description": "A flaw was found in ansible. Credentials, such as secrets, are being disclosed in console log by default and not protected by no_log feature when using those modules. An attacker can take advantage of this information to steal those credentials. The highest threat from this vulnerability is to data confidentiality.", "vulnerabilities": [ { "package": { "ecosystem": "pip", "name": "ansible" }, "severity": "medium",
```


# Update a Dependabot alert

Works with GitHub Apps

You must use an access token with the `security_events` scope to use this endpoint with private repositories. You can also use tokens with the `public_repo` scope for public repositories only. GitHub Apps must have **Dependabot alerts** write permission to use this endpoint.

To use this endpoint, you must have access to security alerts for the repository. For more information, see "Granting access to security alerts."

### Parameters for "Update a Dependabot alert"

#### 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.

**`alert_number`** integer Required

The number that identifies a Dependabot alert in its repository. You can find this at the end of the URL for a Dependabot alert within GitHub, or in `number` fields in the response from the `GET /repos/{owner}/{repo}/dependabot/alerts` operation.

#### Body parameters

**`state`** string Required

The state of the Dependabot alert. A `dismissed_reason` must be provided when setting the state to `dismissed`.

Can be one of: `dismissed`, `open`

**`dismissed_reason`** string

**Required when `state` is `dismissed`.** A reason for dismissing the alert.

Can be one of: `fix_started`, `inaccurate`, `no_bandwidth`, `not_used`, `tolerable_risk`

**`dismissed_comment`** string

`dismissed_comment` string

An optional comment associated with dismissing the alert.

### HTTP response status codes for "Update a Dependabot alert"

| Status code | Description |
| --- | --- |
| 200 | OK |
| 400 | Bad Request |
| 403 | Forbidden |
| 404 | Resource not found |
| 409 | Conflict |
| 422 | Validation failed, or the endpoint has been spammed. |

### Code samples for "Update a Dependabot alert"

PATCH /repos/{owner}/{repo}/dependabot/alerts/{alert_number}

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" \ http(s)://HOSTNAME/api/v3/repos/OWNER/REPO/dependabot/alerts/ALERT_NUMBER \ -d '{"state":"dismissed","dismissed_reason":"tolerable_risk","dismissed_comment":"This alert is accurate but we use a sanitizer."}'
```

### Response

Example response | Response schema

Status: 200


```
{ "number": 2, "state": "dismissed", "dependency": { "package": { "ecosystem": "pip", "name": "django" }, "manifest_path": "path/to/requirements.txt", "scope": "runtime" }, "security_advisory": { "ghsa_id": "GHSA-rf4j-j272-fj86", "cve_id": "CVE-2018-6188", "summary": "Django allows remote attackers to obtain potentially sensitive information by leveraging data exposure from the confirm_login_allowed() method, as demonstrated by discovering whether a user account is inactive", "description": "django.contrib.auth.forms.AuthenticationForm in Django 2.0 before 2.0.2, and 1.11.8 and 1.11.9, allows remote attackers to obtain potentially sensitive information by leveraging data exposure from the confirm_login_allowed() method, as demonstrated by
```