Incomplete validation of cookie attributes

Moderate **bdarnell** published **GHSA-78cv-mqj4-43f7** last month

Package

tornado (pip)

Affected versions

<= 6.5.4

Patched versions

6.5.5

Description

Values passed to the `domain`, `path`, and `samesite` arguments of `RequestHandler.set_cookie` were not completely validated in versions of Tornado prior to 6.5.5. In particular, semicolons would be allowed, which could be used to inject attacker-controlled values for other cookie attributes.

Severity

Moderate 5.4 / 10

CVSS v3 base metrics

Attack vector	Network
Attack complexity	Low
Privileges required	None
User interaction	Required
Scope	Unchanged
Confidentiality	Low
Integrity	Low
Availability	None

Learn more about base metrics

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N

CVE ID

No known CVE

Weaknesses

▶ CWE-74

Credits

DHIRAL2908 Reporter