



USEE & USEE SERVICE SUITE SECURITY UPDATES

5 October 2026





Summary

Arteco has updated **third-party software dependencies to address known security advisories identified during a dependency review**. This notice describes the advisory topics covered by the update and provides the release and customer action details needed to determine whether a deployment requires attention.

The advisory register below **describes vulnerabilities in the upstream packages**. The presence of an affected package does not by itself establish that the vulnerability is exploitable through uSee or uSS. **Product-specific exposure depends on the installed version, configuration and use of the affected functionality**.

Changes included

The development ticket listed advisories as resolved through dependency updates. They concern HTTP request and redirect handling, cookie serialization, request body parsing, wildcard and brace pattern processing, and utility functions. The register provides a short explanation and identifiers for each advisory.



Detailed fixes

1. minimatch ReDoS: nested *() extglobs generate catastrophically backtracking regular expressions

Nested wildcard expressions can trigger excessive regular expression processing and make a process unresponsive.

Product: uSS.

Reference: GHSA-23c5-xmqv-rm74 / CVE-2026-27904

2. axios Vulnerable to Credential Theft and Response Hijacking via Prototype Pollution Gadget in Config Merge

When JavaScript object prototypes have already been modified by another vulnerability, request configuration merging can allow credential theft or response manipulation.

Product: uSS.

Reference: GHSA-3g43-6gmg-66jw / CVE-2026-44495

3. brace-expansion: DoS via exponential-time expansion of consecutive non-expanding {} groups

Certain consecutive brace patterns can take excessive processing time, causing a denial of service.

Product: uSee and uSS.

Reference: GHSA-3jxr-9vmj-r5cp / CVE-2026-13149



4. Axios has a NO_PROXY Hostname Normalization Bypass that Leads to SSRF

Differences in hostname normalization can bypass proxy exclusion rules and create server-side request forgery risks.

Product: uSS.

Reference: GHSA-3p68-rc4w-qgx5 / CVE-2025-62718

5. minimatch has a ReDoS via repeated wildcards with non-matching literal in pattern

Repeated wildcard patterns followed by a non-matching value can cause excessive regular expression processing.

Product: uSS.

Reference: GHSA-3ppc-4f35-3m26 / CVE-2026-26996

6. Axios is Vulnerable to Denial of Service via __proto__ Key in mergeConfig

A specially named configuration key can cause request configuration processing to fail, creating a denial of service risk.

Product: uSS.

Reference: GHSA-43fc-jf86-j433 / CVE-2026-25639



7. Axios' HTTP adapter-streamed uploads bypass maxBodyLength when maxRedirects: 0

Streamed uploads can bypass the configured request body size limit when redirect handling is disabled.

Product: uSS.

Reference: GHSA-5c9x-8gcm-mpgx / CVE-2026-42034

8. Axios: unbounded recursion in toFormData causes DoS via deeply nested request data

Deeply nested request data can cause excessive recursion during form-data conversion, disrupting the process.

Product: uSS.

Reference: GHSA-62hf-57xw-28j9 / CVE-2026-42039

9. Axios: Header Injection via Prototype Pollution

In a process with an already modified object prototype, inherited values can inject unexpected HTTP request headers.

Product: uSS.

Reference: GHSA-6chq-wfr3-2hj9 / CVE-2026-42035



10. Axios: Nested axios option objects can consume polluted prototype values

Nested authentication and query serialization options can consume inherited values from an already modified object prototype, changing outgoing requests.

Product: uSS.

Reference: GHSA-7q8q-rj6j-mhjg / CVE-2026-67319

11. minimatch has ReDoS: matchOne() combinatorial backtracking via multiple non-adjacent GLOBSTAR segments

Patterns containing multiple recursive wildcard segments can require excessive matching time and block processing.

Product: uSS.

Reference: GHSA-7r86-cg39-jmmj / CVE-2026-27903

12. axios has DoS & Header Injection via Prototype Pollution Read-Side Gadgets in axios merge functions

Inherited values from an already modified object prototype can affect configuration merging, causing failures or unexpected headers.

Product: uSS.

Reference: GHSA-898c-q2cr-xwhg / CVE-2026-44490

13. lodash vulnerable to Prototype Pollution via array path bypass in `_.unset` and `_.omit`

Array-based property paths can bypass protections in property removal functions and allow JavaScript object prototype modification.

Product: uSS.

Reference: GHSA-f23m-r3pf-42rh / CVE-2026-2950



14. brace-expansion: Zero-step sequence causes process hang and memory exhaustion

A sequence with a zero increment can cause a process to hang or exhaust memory during brace expansion.

Product: uSS.

Reference: GHSA-f886-m6hf-6m8v / CVE-2026-33750

15. Axios has Unrestricted Cloud Metadata Exfiltration via Header Injection Chain

A chain involving header injection can allow retrieval and disclosure of cloud instance metadata under affected request conditions.

Product: uSS.

Reference: GHSA-fvcv-3m26-pcqx / CVE-2026-40175

16. Axios: Regular Expression Denial of Service (ReDoS) via Cookie Name Injection

An attacker-controlled cookie name can trigger excessive regular expression processing in cookie handling.

Product: uSS.

Reference: GHSA-hfxv-24rg-xrqf / CVE-2026-44496



17. Axios proxy credentials can leak when a redirected request changes to a direct connection

With authenticated proxies and automatic redirects in Node.js, proxy credentials can be forwarded to a redirect destination when the connection changes to direct.

Product: uSS.

Reference: GHSA-j5f8-grm9-p9fc / CVE-2026-44486

18. axios Requests Vulnerable To Possible SSRF and Credential Leakage via Absolute URL

An absolute URL can override the intended base URL in affected request handling, allowing requests to unintended destinations and possible credential leakage.

Product: uSS.

Reference: GHSA-jr5f-v2jv-69x6 / CVE-2025-27152

19. Axios: no_proxy bypass via IP alias allows SSRF

Proxy exclusion matching can treat loopback IP addresses and equivalent hostnames differently, creating unintended request routing and SSRF risks.

Product: uSS.

Reference: GHSA-m7pr-hjqh-92cm / CVE-2026-42038



20. brace-expansion: DoS via unbounded expansion length causing an out-of-memory process crash

Brace expansion can generate excessively long output and exhaust process memory even when the number of results is limited.

Product: uSee and uSS.

Reference: GHSA-mh99-v99m-4gvg / CVE-2026-14257

21. Axios: Prototype pollution gadgets can alter axios request construction

An already modified object prototype can influence request construction and alter the resulting outgoing request.

Product: uSS.

Reference: GHSA-mmx7-hfxj-jppx / CVE-2026-67316

22. Axios: Proxy-Authorization Credential Leak to Origin Server Across HTTP-to-HTTPS Redirect in Axios Node.js HTTP Adapter

In affected Node.js proxy and redirect configurations, proxy authentication credentials can reach an origin server after an HTTP-to-HTTPS redirect.

Product: uSS.

Reference: GHSA-p92q-9vqr-4j8v / CVE-2026-44487



23. Axios: Prototype Pollution Gadgets - Response Tampering, Data Exfiltration, and Request Hijacking

An already modified object prototype can influence request and response handling, enabling response manipulation, data disclosure or redirected requests.

Product: uSS.

Reference: GHSA-pf86-5x62-jrwf / CVE-2026-42033

24. axios's shouldBypassProxy does not recognize IPv4-mapped IPv6 addresses, allowing NO_PROXY bypass (incomplete fix for CVE-2025-62718)

Proxy exclusion logic can fail to recognize IPv4 addresses represented in IPv6 format, bypassing expected routing rules.

Product: uSS.

Reference: GHSA-pjwm-pj3p-43mv / CVE-2026-44492

25. Axios: Incomplete Fix for CVE-2025-62718 — NO_PROXY Protection Bypassed via RFC 1122 Loopback Subnet (127.0.0.0/8) in Axios 1.15.0

Proxy exclusion handling can fail for alternative addresses within the IPv4 loopback range, leaving an earlier fix incomplete.

Product: uSS.

Reference: GHSA-pmwg-cvhr-8vh7 / CVE-2026-42043



26. cookie accepts cookie name, path, and domain with out of bounds characters

Insufficient validation of cookie names, domains and paths can allow invalid characters to alter serialized cookie attributes.

Product: uSS.

Reference: GHSA-pxg6-pf52-xh8x / CVE-2024-47764

27. follow-redirects leaks Custom Authentication Headers to Cross-Domain Redirect Targets

Custom authentication headers can be forwarded to another domain during automatic redirects, exposing sensitive authentication information.

Product: uSS.

Reference: GHSA-r4q5-vmmm-2653

28. lodash vulnerable to Code Injection via _.template imports key names

Untrusted import names passed into template compilation can cause code injection; inherited keys can also matter when object prototypes are already modified.

Product: uSS.

Reference: GHSA-r5fr-rjxr-66jc / CVE-2026-4800



29. brace-expansion: DoS via unbounded intermediate arrays, bypassing the CVE-2026-14257 mitigation

Intermediate expansion arrays can evade earlier output limits, causing excessive memory use or prolonged processing.

Product: uSS.

Reference: GHSA-rgw5-rvv9-x895 / CVE-2026-69152

30. body-parser vulnerable to denial of service when invalid limit value silently disables size enforcement

An invalid request size limit configuration can silently disable size enforcement and expose the process to oversized request bodies.

Product: uSee and uSS.

Reference: GHSA-v422-hmww-36x6 / CVE-2026-12590

31. Axios: HTTP adapter streamed responses bypass maxContentLength

Streamed HTTP responses can bypass the configured maximum response content length.

Product: uSS.

Reference: GHSA-vf2m-468p-8v99 / CVE-2026-42036



32. Axios authentication checks can be bypassed through polluted validateStatus configuration

An already modified object prototype can influence response status validation. Applications relying on that result for authentication decisions may be affected.

Product: uSS.

Reference: GHSA-w9j2-pvgh-6h63 / CVE-2026-42041

33. Axios Cross-Site Request Forgery Vulnerability

Affected cross-origin request behavior can expose a cross-site request forgery token to another origin.

Product: uSS.

Reference: GHSA-wf5p-g6vw-rhxx / CVE-2023-45857

34. Axios: Null Byte Injection via Reverse-Encoding in AxiosURLSearchParams

Certain URL parameter encoding behavior can introduce null bytes, potentially causing differences in how downstream systems interpret a request.

Product: uSS.

Reference: GHSA-xhjh-pmcv-23jw / CVE-2026-42040



35. Axios: XSRF Token Cross-Origin Leakage via Prototype Pollution Gadget in withXSRFToken Boolean Coercion

An already modified object prototype can affect the decision to attach a cross-site request forgery token, allowing leakage across origins.

Product: uSS.

Reference: GHSA-xx6v-rp6x-q39c / CVE-2026-42042

36. Lodash has Prototype Pollution Vulnerability in `_.unset` and `_.omit` functions

Property removal functions can modify JavaScript object prototypes through affected property paths.

Product: uSS.

Reference: GHSA-xxjr-mmjv-4gpg / CVE-2025-13465

37. @nestjs/microservices CVE-2026-102281

A deeply nested microservice message pattern can terminate the receiving process.

Product: uSS.

Reference: CVE-2026-102281 / GHSA-m8vh-jmq9-5rjg.

38. engine.io CVE-2026-102599

A protocol revision mismatch can cause denial of service in Engine.IO

Product: uSS.

Reference: CVE-2026-102599 / GHSA-2gc4-cqfq-p2gv.



39. fast-uri CVE-2026-86472

Percent-encoded hostname characters can cause inconsistent case normalization and differences in hostname interpretation.

Product: uSS.

Reference: CVE-2026-86472 / GHSA-hrr3-gc8f-f4qj.

40. moment CVE-2026-17495

A crafted non-string locale name can cause path traversal during locale handling.

Product: uSS.

Reference: CVE-2026-17495 / GHSA-4p3w-j4w9-5jqw.

41. undici CVE-2026-85024

An error while processing compressed WebSocket messages can cause denial of service.

Product: uSS Launcher.

Reference: CVE-2026-85024.

42. multer CVE-2026-88932

An aborted upload can leave orphaned disk writes, creating a denial of service risk. NestJS platform-express is also flagged because it depends on the affected Multer version.

Product: uSS.

Reference: CVE-2026-88932.



43. multer CVE-2026-77078

Crafted multipart field names can disrupt upload processing and cause denial of service.

Product: uSS.

Reference: CVE-2026-77078 / GHSA-wc9g-mqfw-jrwm.

44. multer CVE-2026-77037

Aborted uploads can leak file descriptors and exhaust process resources.

Product: uSS.

Reference: CVE-2026-77037 / GHSA-qfvm-cv95-jqjf.

45. multer CVE-2026-77063

An asynchronous file filter race condition can bypass upload file size limits.

Product: uSS.

Reference: CVE-2026-77063 / GHSA-qvfw-j98x-7q72.

46. multer CVE-2026-82333

Oversized array indices in multipart field names can cause denial of service.

Product: uSS.

Reference: CVE-2026-82333 / GHSA-535w-7cp7-47q4.



47. browserslist CVE-2026-73089

Distinct query results can accumulate without cache eviction and eventually exhaust process memory.

Product: uSee and uSS.

Reference: CVE-2026-73089 / GHSA-c83g-rgw3-j3cx.

48. browserslist CVE-2026-73088

Untrusted custom statistics can cause a crash or writes to JavaScript object prototypes.

Product: uSee and uSS.

Reference: CVE-2026-73088 / GHSA-73wf-gq98-2v4g.

49. fast-uri CVE-2026-75931

Skipped internationalized domain name normalization on scheme-relative references can cause hostname confusion.

Product: uSS.

Reference: CVE-2026-75931 / GHSA-5jgf-p345-68v8.

50. fast-uri CVE-2026-75975

Malformed IPv6 normalization can create server-side request forgery risks.

Product: uSS.

Reference: CVE-2026-75975 / GHSA-f65p-4m7j-42xc.



51. fast-uri CVE-2026-75899

Repeated percent-decoding of a hostname can create server-side request forgery risks.

Product: uSS.

Reference: CVE-2026-75899 / GHSA-fph4-wmhf-6fwf.

52. fast-uri CVE-2026-76172

Percent-encoded scheme normalization can cause hostname confusion.

Product: uSS.

Reference: CVE-2026-76172 / GHSA-jqff-g426-hqxp.

53. qs CVE-2026-82562

Bracket-key comma parsing can bypass configured array limits.

Product: uSS.

Reference: CVE-2026-82562 / GHSA-x5fp-wj9c-mxmx.

54. qs CVE-2026-82417

An attacker-controlled isBuffer value can cause denial of service.

Product: uSee and uSS.

Reference: CVE-2026-82417 / GHSA-4mjr-xmp4-gh2g.