



IGL-Technologies eParking.fi Missing Authentication for Critical Function

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

| | |
|------------------------|---|
| CVE | CVE-2026-29796 |
| State | PUBLISHED |
| Assigner | icscert |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2026-03-20 23:16:43 UTC |
| Updated | 2026-05-13 16:33:23 UTC |
| Description | WebSocket endpoints lack proper authentication mechanisms, enabling attackers to perform unauthorized station impersonation |

Risk And Classification

Primary CVSS: v4.0 9.3 CRITICAL from ics-cert@hq.dhs.gov

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:L/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

EPSS: 0.000590000 probability, percentile 0.185420000 (date 2026-05-15)

Problem Types: CWE-306 | CWE-306 CWE-306

| Version | Source | Type | Score | Severity | Vector |
|---------|---------------------|-----------|-------|----------|--|
| 4.0 | ics-cert@hq.dhs.gov | Secondary | 9.3 | CRITICAL | CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:L/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X |
| 4.0 | CNA | CVSS | 9.3 | CRITICAL | CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:L/SC:N/SI:N/SA:N |
| 3.1 | nvd@nist.gov | Primary | 9.8 | CRITICAL | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H |
| 3.1 | ics-cert@hq.dhs.gov | Secondary | 9.4 | CRITICAL | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:L |
| 3.1 | CNA | CVSS | 9.4 | CRITICAL | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:L |

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

Privileges Required

None

User Interaction

None

Confidentiality

High

Integrity

High

Availability

Low

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:L/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX:MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|-------------|--------|-------------|---------|--------|---------|----------|
| Application | lgl | Eparking.fi | - | All | All | All |

Vendor Declared Affected Products

Vendor Declared Affected Products

| Source | Vendor | Product | Version | Platforms |
|--------|----------------------------------|-----------------------------|------------------------------|---------------|
| CNA | IGL-Technologies | EParking.fi | affected All versions custom | Not specified |

References

| Reference | Source | Link | Tags |
|---|--|---|---------------------|
| www.cisa.gov/news-events/ics-advisories/icsa-26-078-08 | ics-cert@hq.dhs.gov | www.cisa.gov | Not Applicable |
| github.com/cisagov/CSAF/blob/develop/csaf_files/OT/white/2026/icsa-26-07... | ics-cert@hq.dhs.gov | github.com | Not Applicable |
| CVE Program record | CVE.ORG | www.cve.org | canonical |
| NVD vulnerability detail | NVD | nvd.nist.gov | canonical, analysis |

Vendor Comments And Credit

Discovery Credit

CNA: Khaled Sarieedine and Mohammad Ali Sayed reported this vulnerability to CISA. (en)

Additional Advisory Data

Solutions

CNA: IGL-Technologies has updated eParking's OCPP servers to reduce the risks posed by the vulnerability. These updates implemented the following security controls: 1-Enforce modern security profiles and stronger authentication. 2-Device level whitelisting was implemented to ensure authorized devices connect. 3-Rate limiting controls prevent excessive requests and reduces denial-of-service attacks. 4-Enhanced automated monitoring and alerting to detection abnormal network activity. Devices using the encrypted deployment of eParking's OCPP servers or IGL-Technologies proprietary eTolppa protocol are not impacted by these vulnerabilities.

CNA: To prevent this in the future IGL-Technologies will continue vulnerability monitoring under their ISO 27001:2022 security program and tighten security requirements for future third-party OCPP hardware approvals.

CNA: For more information please contact the IGL-Technologies security team at this email address: security@igl.fi. <mailto:security@igl.fi>

There are currently no legacy QID mappings associated with this CVE.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report