



# IGL-Technologies eParking.fi Improper Restriction of Excessive Authentication Attempts

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

## Summary

<b>CVE</b>	CVE-2026-31903
<b>State</b>	PUBLISHED
<b>Assigner</b>	icscert
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-03-20 23:16:43 UTC
<b>Updated</b>	2026-05-06 18:10:44 UTC
<b>Description</b>	The WebSocket Application Programming Interface lacks restrictions on the number of authentication requests. This absence

## Risk And Classification

**Primary CVSS:** v4.0 8.7 HIGH from ics-cert@hq.dhs.gov

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/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

**Problem Types:** CWE-307 | CWE-307 CWE-307 | CWE-307 CWE-307 Improper Restriction of Excessive Authentication Attempts

Version	Source	Type	Score	Severity	Vector
4.0	ics-cert@hq.dhs.gov	Secondary	8.7	HIGH	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N/E:X
4.0	CNA	CVSS	8.7	HIGH	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N
3.1	ics-cert@hq.dhs.gov	Secondary	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
3.1	CNA	CVSS	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

## CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

None

Confidentiality

None

Integrity

None

Availability

High

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/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

### CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

High

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

Source	Vendor	Product	Version	Platforms
--------	--------	---------	---------	-----------

CNA	<a href="#">IGL-Technologies</a>	<a href="#">EParking.fi</a>	affected All versions custom	Not specified
-----	----------------------------------	-----------------------------	------------------------------	---------------

## References

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

## Vendor Comments And Credit

### Discovery Credit

**CNA:** Khaled Sarieddine 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.

**CNA:** 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). <mailto:security@igl.fi>

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

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

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](https://cve.report/api)

CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)