



# CVE-2020-3371

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

## Summary

<b>CVE</b>	CVE-2020-3371
<b>State</b>	PUBLIC
<b>Assigner</b>	psirt@cisco.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2020-11-06 19:15:00 UTC
<b>Updated</b>	2023-11-07 03:22:00 UTC
<b>Description</b>	A vulnerability in the web UI of Cisco Integrated Management Controller (IMC) could allow an authenticated, remote attacker

## Risk And Classification

**Problem Types: CWE-78**

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Integrated Management Controller	All	All	All	All
Application	Cisco	Integrated Management Controller	All	All	All	All

## References

Reference	Source	Link	Tags
Cisco Integrated Management Controller Command Injection Vulnerability	CISCO	<a href="https://tools.cisco.com">tools.cisco.com</a>	Vendor Advisory
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

No vendor comments have been submitted for this CVE.

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](#).

**CVE.report and Source URL Uptime Status [status.cve.report](#)**