



# CVE-2020-10917

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

## Summary

<b>CVE</b>	CVE-2020-10917
<b>State</b>	PUBLIC
<b>Assigner</b>	zdi-disclosures@trendmicro.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2020-07-22 23:15:00 UTC
<b>Updated</b>	2020-07-28 17:01:00 UTC
<b>Description</b>	This vulnerability allows remote attackers to execute arbitrary code on affected installations of NEC ESMPRO Manager 6.4:

## Risk And Classification

**Problem Types:** CWE-502

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Nec</a>	<a href="#">Esmpro Manager</a>	6.42	All	All	All
Application	<a href="#">Nec</a>	<a href="#">Esmpro Manager</a>	6.42	All	All	All

## References

Reference	Source	Link	Tags
ZDI-20-684   Zero Day Initiative	MISC	<a href="http://www.zerodayinitiative.com">www.zerodayinitiative.com</a>	Third Party Advisory, VDB Entry
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="http://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](#)**