CVE-2020-6092

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2020-6092
State	PUBLIC
Assigner	talos-cna@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-05-18 17:15:00 UTC
Updated	2022-05-12 17:21:00 UTC
Description	An exploitable code execution vulnerability exists in the way Nitro Pro 13.9.1.155 parses Pattern objects. A specially craftec

Risk And Classification

Problem Types: CWE-190

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Gonitro	Nitro Pro	13.9.1.155	All	All	All
Application	Gonitro	Nitro Pro	13.9.1.155	All	All	All

References

Reference	Source	Link	Tags
TALOS-2020-1013 || Cisco Talos Intelligence Group - Comprehensive Threat Intelligence	MISC	talosintelligence.com	Exploit, Thirc
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, ar

No vendor comments have been submitted for this CVE.

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

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