CVE-2019-16278

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2019-16278
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-10-14 17:15:00 UTC
Updated	2023-03-23 18:11:00 UTC
Description	Directory Traversal in the function http_verify in nostromo nhttpd through 1.9.6 allows an attacker to achieve remote code e

Risk And Classification

EPSS: 0.943930000 probability, percentile 0.999740000 (date 2026-05-11)

CISA KEV: Listed on 2024-11-07; due 2024-11-28; ransomware use Unknown

Problem Types: CWE-22

CISA Known Exploited Vulnerability

Vendor	Nostromo
Product	nhttpd
Name	Nostromo nhttpd Directory Traversal Vulnerability
Required Action	Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.
Notes	https://www.nazgul.ch/dev/nostromo_cl.txt ; https://nvd.nist.gov/vuln/detail/CVE-2019-16278

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Nazgul	Nostromo Nhttpd	All	All	All	All

References

Reference	Source	Link	Tags
sp0re	MISC	sp0re.sh	Not Applicable
www.nazgul.ch/dev/nostromo_cl.txt	MISC	www.nazgul.ch	Release Notes,
404 Not Found	MISC	git.sp0re.sh	Exploit, Third P
Nostromo 1.9.6 Directory Traversal / Remote Command Execution ≈ Packet Storm	MISC	packetstormsecurity.com	

nostromo 1.9.6 Remote Code Execution ≈ Packet Storm	MISC	packetstormsecurity.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analy
CISA Known Exploited Vulnerabilities catalog	CISA	www.cisa.gov	kev

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

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