



CVE-2016-8591

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

Summary

CVE	CVE-2016-8591
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-04-28 19:59:00 UTC
Updated	2017-05-11 01:29:00 UTC
Description	log_query.cgi in Trend Micro Threat Discovery Appliance 2.6.1062r1 and earlier allows remote authenticated users to execute arbitrary commands via the log_query.cgi script.

Risk And Classification

Problem Types: CWE-264

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Trendmicro	Threat Discovery Appliance	All	r1	All	All

References

Reference	Source	Link
Trend Micro Threat Discovery Appliance 2.6.1062r1 log_query.cgi Remote Code Execution ≈ Packet Storm	MISC	packetstormsecurity.com
Trend Micro Threat Discovery Appliance CVE-2016-8591 Command Injection Vulnerability	BID	www.securityfocus.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

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](#).

Free CVE JSON API cve.report/api

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