CVE-2015-1187

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

Summary

CVE	CVE-2015-1187
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-09-21 16:29:00 UTC
Updated	2026-04-21 18:55:58 UTC
Description	The ping tool in multiple D-Link and TRENDnet devices allow remote attackers to execute arbitrary code via the ping_addr

Risk And Classification

Primary CVSS: v3.1 9.8 CRITICAL from nvd@nist.gov

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

EPSS: 0.828850000 probability, percentile 0.992540000 (date 2026-04-22)

CISA KEV: Listed on 2022-03-25; due 2022-04-15; ransomware use Unknown

Problem Types: CWE-287 | n/a | CWE-287 CWE-287 Improper Authentication

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	ADP	DECLARED	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
2.0	nvd@nist.gov	Primary	10		AV:N/AC:L/Au:N/C:C/I:C/A:C

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

AV:N/AC:L/Au:N/C:C/I:C/A:C

CISA Known Exploited Vulnerability

Vendor	D-Link and TRENDnet
Product	Multiple Devices
Name	D-Link and TRENDnet Multiple Devices Remote Code Execution Vulnerability
Required Action	The impacted product is end-of-life and should be disconnected if still in use.
Notes	https://nvd.nist.gov/vuln/detail/CVE-2015-1187

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Dlink	Dir-626l	-	All	All	All
Operating System	Dlink	Dir-626l Firmware	1.04	b04	All	All
Hardware	Dlink	Dir-636l	-	All	All	All
Operating System	Dlink	Dir-636l Firmware	1.04	All	All	All
Hardware	Dlink	Dir-808l	-	All	All	All
Operating System	Dlink	Dir-808l Firmware	1.03	b05	All	All

Hardware	Dlink	Dir-810l	-	All	All	All
Operating System	Dlink	Dir-810l Firmware	1.01	b04	All	All
Operating System	Dlink	Dir-810l Firmware	2.02	b01	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference	Source
D-Link Technical Support	af854a3a-2127-422b-91ae-364da
www.cisa.gov/known-exploited-vulnerabilities-catalog	134c704f-9b21-4f2e-91b3-4a4673
D-Link DIR-636L CVE-2015-1187 Remote Command Injection and Authentication Bypass Vulnerabilities	af854a3a-2127-422b-91ae-364da
Full Disclosure: CVE-2015-1187: D-Link DIR-636L Remote Command Injection - Incorrect Authentication	af854a3a-2127-422b-91ae-364da
D-Link/TRENDnet NCC Service Command Injection ≈ Packet Storm	af854a3a-2127-422b-91ae-364da
D-Link DIR636L Remote Command Injection ≈ Packet Storm	af854a3a-2127-422b-91ae-364da
secpub/Multivendor/ncc2 at master · darkarnium/secpub · GitHub	af854a3a-2127-422b-91ae-364da
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD
CISA Known Exploited Vulnerabilities catalog	CISA

No vendor comments have been submitted for this CVE.

Additional Advisory Data

Source	Time	Event
ADP	2022-03-25T00:00:00.000Z	CVE-2015-1187 added to CISA KEV

Legacy QID Mappings

379469 For Vulnerability CVE-2015-1187

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