

CVE-2021-27137

DD-WRT Stack-Based Buffer Overflow Vulnerability

CISA KEV since Jul 21, 2026

Actively exploited

An issue was discovered in router/upnp/src/ssdp.c in DD-WRT before 45724. An unsafe strcpy in the UPnP handling functionality allows an unauthenticated remote attacker to send a request that would overflow an internal fixed buffer. Exploitation requires the DD-WRT user to enable UPnP (which is off by default, and only listens on internal interfaces by default). This occurs in ssdp_msearch (reachable by an M-SEARCH request).

EVRS 75 / ₁₀₀ Urgent priority	CVSS V3.1 8.1 High · NVD	EPSS 0.040 90.5th percentile · FIRST	CISA DEADLINE Jul 24, 2026 CISA federal deadline · Overdue by 3 months
---	--	--	--

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☐ KEV recency	Added to CISA KEV within the last year
☒ EPSS	0.040 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 8.1	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified

CISA required action: Apply mitigations in accordance with vendor instructions, ensuring compliance with CISA's BOD 26-04 Prioritizing Security Updates Based on Risk (see URL in Notes) guidance and CISA's "Forensics Triage Requirements" (see URL in Notes). Follow applicable BOD 26-04 guidance for cloud services or discontinue use of the product if mitigations are unavailable. Stakeholders are responsible for evaluating each asset's internet exposure and ensuring adherence to BOD 26-04 patching guidelines. **CISA note:** This vulnerability affects a common open-source component, third-party library, proprietary implementation, or a protocol used by different products. Please check with specific vendors for information on patching status.
Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
dd-wrt	< 45724	45724	NVD

Sources

Vendor guidance	github.com/advisories/GHSA-qx3v-2jx6-8m2c	svn.dd-wrt.com	svn.dd-wrt.com/changeset/45724
BOD 26-04	cisa.gov/news-events/directives/bod-26-04-prioritizing-security-updates-based-risk	Forensics Triage Requirements	cisa.gov/news-events/directives/bod-26-04-implementation-guidance-prioritizing-security-updates-based-risk
NVD	nvd.nist.gov/vuln/detail/CVE-2021-27137	CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2021-34854	Current data	evulnable.com/vulnerability-management/cve/CVE-2021-27137

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.