CVE-2014-8361

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2014-8361
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-05-01 15:59:00 UTC
Updated	2023-09-05 22:15:00 UTC
Description	The miniigd SOAP service in Realtek SDK allows remote attackers to execute arbitrary code via a crafted NewInternalClien

Risk And Classification

EPSS: 0.938930000 probability, percentile 0.998730000 (date 2026-04-02)

CISA KEV: Listed on 2023-09-18; due 2023-10-09; ransomware use Unknown

Problem Types: CWE-20

CISA Known Exploited Vulnerability

Vendor	Realtek
Product	SDK
Name	Realtek SDK Improper Input Validation Vulnerability
Required Action	Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.
Notes	https://web.archive.org/web/20150831100501/http://securityadvisories.dlink.com/security/publication.aspx?name=SAP10055; https://nvd.nist.gov/vuln/detail/CVE-2014-8361

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	D-link	Dir-600l	a1	All	All	All
Hardware	D-link	Dir-600l	b1	All	All	All
Hardware	D-link	Dir-600l	a1	All	All	All
Hardware	D-link	Dir-600l	b1	All	All	All
Operating System	D-link	Dir-600l Firmware	All	All	All	All
Operating System	D-link	Dir-600l Firmware	All	All	All	All
Hardware	D-link	Dir-605l	a1	All	All	All

Hardware	D-link	Dir-605l	b1	All	All	All
Hardware	D-link	Dir-605l	a1	All	All	All
Hardware	D-link	Dir-605l	b1	All	All	All
Operating System	D-link	Dir-605l Firmware	All	All	All	All
Operating System	D-link	Dir-605l Firmware	All	All	All	All
Hardware	D-link	Dir-619l	a1	All	All	All
Hardware	D-link	Dir-619l	b1	All	All	All
Hardware	D-link	Dir-619l	a1	All	All	All
Hardware	D-link	Dir-619l	b1	All	All	All
Operating System	D-link	Dir-619l Firmware	All	All	All	All
Operating System	D-link	Dir-619l Firmware	All	All	All	All
Hardware	D-link	Dir-809	a1	All	All	All
Hardware	D-link	Dir-809	a2	All	All	All
Hardware	D-link	Dir-809	a1	All	All	All
Hardware	D-link	Dir-809	a2	All	All	All
Operating System	D-link	Dir-809 Firmware	All	All	All	All
Hardware	D-link	Dir-905l	a1	All	All	All
Hardware	D-link	Dir-905l	a1	All	All	All
Operating System	D-link	Dir-905l Firmware	All	All	All	All
Hardware	Dlink	Dir-600l	a1	All	All	All
Hardware	Dlink	Dir-600l	b1	All	All	All
Operating System	Dlink	Dir-600l Firmware	All	All	All	All
Operating System	Dlink	Dir-600l Firmware	All	All	All	All
Hardware	Dlink	Dir-605l	a1	All	All	All
Hardware	Dlink	Dir-605l	b1	All	All	All
Operating System	Dlink	Dir-605l Firmware	All	All	All	All
Operating System	Dlink	Dir-605l Firmware	All	All	All	All
Hardware	Dlink	Dir-619l	a1	All	All	All
Hardware	Dlink	Dir-619l	b1	All	All	All
Operating System	Dlink	Dir-619l Firmware	All	All	All	All
Operating System	Dlink	Dir-619l Firmware	All	All	All	All
Hardware	Dlink	Dir-809	a1	All	All	All
Hardware	Dlink	Dir-809	a2	All	All	All
Operating System	Dlink	Dir-809 Firmware	All	All	All	All
Hardware	Dlink	Dir-905l	a1	All	All	All
Operating System	Dlink	Dir-905l Firmware	All	All	All	All

Operating System	Dlink	Dir-905l Firmware	All	All	All	All
Application	Realtek	Realtek Sdk	-	All	All	All
Application	Realtek	Realtek Sdk	-	All	All	All

References

Reference	Source	Link	Tags
Realtek rtl81xx SDK CVE-2014-8361 Remote Code Execution Vulnerability	BID	www.securityfocus.com	Third Party Advis
D-Link Technical Support	MISC	web.archive.org	
New HinataBot Exploits CVE-2014-8361 in DDoS Attacks	MISC	sensorstechforum.com	
Realtek SDK - Miniigd UPnP SOAP Command Execution (Metasploit)	EXPLOIT-DB	www.exploit-db.com	Third Party Advis
D-Link Technical Support	CONFIRM	securityadvisories.dlink.com	Vendor Advisory
Realtek SDK Miniigd UPnP SOAP Command Execution ≈ Packet Storm	MISC	packetstormsecurity.com	Third Party Advis
Zero Day Initiative	MISC	www.zerodayinitiative.com	Third Party Advis
JVN#67456944: Multiple vulnerabilities in multiple Aterm products	JVN	jvn.jp	
JVN#47580234: Multiple vulnerabilities in multiple ELECOM products	JVN	jvn.jp	Third Party Advis
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analys
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.