



CVE-2014-2994

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

Summary

CVE	CVE-2014-2994
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-04-27 04:32:01 UTC
Updated	2026-05-06 22:30:45 UTC
Description	Stack-based buffer overflow in Acunetix Web Vulnerability Scanner (WVS) 8 build 20120704 allows remote attackers to ex

Risk And Classification

Primary CVSS: v2.0 10 from nvd@nist.gov

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

Problem Types: CWE-119 | n/a

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Acunetix	Web Vulnerability Scanner	8	build_20120704	All	All

Vendor Declared Affected Products				
Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified
References				
Reference		Source	Link	
Acunetix 8 build 20120704 - Remote Stack Based Overflow		af854a3a-2127-422b-91ae-364da2661108	www.exploit-db.com	
An7i Security: Pwn the n00bs - Acunetix 0day		af854a3a-2127-422b-91ae-364da2661108	an7isec.blogspot.co.il	
Acunetix 8 Stack Buffer Overflow ≈ Packet Storm		af854a3a-2127-422b-91ae-364da2661108	packetstormsecurity.co	
Pwning Script Kiddies – Acunetix Buffer Overflow Blog of Osanda		af854a3a-2127-422b-91ae-364da2661108	osandamalith.wordpress	
Acunetix Web Vulnerability Scanner Buffer Overflow Exploit - YouTube		af854a3a-2127-422b-91ae-364da2661108	www.youtube.com	
Acunetix 8 Scanner Buffer Overflow ≈ Packet Storm		af854a3a-2127-422b-91ae-364da2661108	packetstormsecurity.co	
Misleading Reports of 0-Day in Acunetix WVS Acunetix		af854a3a-2127-422b-91ae-364da2661108	www.acunetix.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.				