



GarrettCom Magnum 6K and 10K Authentication Bypass via Hardcoded String

MITRE

NVD

CVE.ORG

JSON API

Print: PDF

Summary	
CVE	CVE-2017-20234
State	PUBLISHED
Assigner	VulnCheck
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-03 23:17:00 UTC
Updated	2026-04-07 13:20:55 UTC
Description	GarrettCom Magnum 6K and 10K managed switches contain an authentication bypass vulnerability that allows unauthentic

Risk And Classification

Primary CVSS: v4.0 9.3 CRITICAL from disclosure@vulncheck.com

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

EPSS: 0.000230000 probability, percentile 0.061560000 (date 2026-04-07)

Problem Types: CWE-798 | CWE-798 CWE-798 Use of Hard-coded Credentials

Version	Source	Type	Score	Severity	Vector
4.0	disclosure@vulncheck.com	Secondary	9.3	CRITICAL	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X
4.0	CNA	CVSS	9.3	CRITICAL	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X
3.1	disclosure@vulncheck.com	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	CNA	CVSS	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v4.0 Breakdown	
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None

User Interaction

None

Confidentiality

High

Integrity

High

Availability

High

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSG:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Belden	GarrettCom Magnum 6K And 10K Managed Switches	affected 4.6.0 semver	Not specified
CNA	Belden	GarrettCom Magnum 6K And 10K Managed Switches	affected 4.7.6 semver	Not specified
CNA	Belden	GarrettCom Magnum 6K And 10K Managed Switches	unaffected 4.7.7 semver	Not specified

References		
Reference	Source	Link
www.vulncheck.com/advisories/garrettcom-magnum-6k-and-10k-authentication-bypass...	disclosure@vulncheck.com	www.vulncheck.com
assets.belden.com/m/114be964b4651983/original/Security-Bulletin-MNS-6K-10K-Garr...	disclosure@vulncheck.com	assets.belden.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.		