CVE-2020-25223

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2020-25223
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-09-25 04:23:00 UTC
Updated	2023-10-17 17:15:00 UTC
Description	A remote code execution vulnerability exists in the WebAdmin of Sophos SG UTM before v9.705 MR5, v9.607 MR7, and v9

Risk And Classification

EPSS: 0.942930000 probability, percentile 0.999420000 (date 2026-04-01)

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

Problem Types: CWE-78

CISA Known Exploited Vulnerability

Vendor	Sophos
Product	SG UTM
Name	Sophos SG UTM Remote Code Execution Vulnerability
Required Action	Apply updates per vendor instructions.
Notes	https://nvd.nist.gov/vuln/detail/CVE-2020-25223

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Sophos	Unified Threat Management	All	All	All	All
Application	Sophos	Unified Threat Management	9.511	-	All	All
Application	Sophos	Unified Threat Management	9.607	-	All	All
Application	Sophos	Unified Threat Management	9.705	-	All	All
Application	Sophos	United Threat Management	All	All	All	All
Application	Sophos	United Threat Management	9.511	-	All	All
Application	Sophos	United Threat Management	9.607	-	All	All
Application	Sophos	United Threat Management	9.705	-	All	All

Application	Sophos	United Threat Management	All	All	All	All
Application	Sophos	United Threat Management	9.511	-	All	All
Application	Sophos	United Threat Management	9.607	-	All	All
Application	Sophos	United Threat Management	9.705	-	All	All

References

Reference
Advisory: Resolved RCE in SG UTM WebAdmin (CVE-2020-25223) - Community Security Blog - Sophos Community - Sophos Community
Community Security Blog - Sophos Community - Sophos Community
Sophos UTM Creating a 'Big' Bounty with Remote Code Execution Flaw - SecPod Blog
CWE - CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') (4.9)
Sophos UTM WebAdmin SID Command Injection ≈ Packet Storm
CVE Program record
NVD vulnerability detail
CISA Known Exploited Vulnerabilities catalog

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

379219 Sophos UTM Remote Code Execution (RCE) Vulnerability

730598 Sophos SG UTM Remote Code Execution (RCE) Vulnerability (sophos-sa-20200918-sg-webadmin-rce)