

CVE-2017-5689

Intel Active Management Technology (AMT), Small Business Technology (SBT), and Standard Manageability Privilege Escalation Vulnerability

Exigent

CISA KEV since Jan 28, 2022

Actively exploited

Public exploit module (Metasploit)

An unprivileged network attacker could gain system privileges to provisioned Intel manageability SKUs: Intel Active Management Technology (AMT) and Intel Standard Manageability (ISM). An unprivileged local attacker could provision manageability features gaining unprivileged network or local system privileges on Intel manageability SKUs: Intel Active Management Technology (AMT), Intel Standard Manageability (ISM), and Intel Small Business Technology (SBT).

EVRS

85/100

Immediate priority

CVSS V3.1

9.8

Critical · NVD

EPSS

0.922

99.82nd percentile · FIRST

CISA DEADLINE

Jul 28, 2022

KEV since 2022 · listed over a year

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	On the CISA KEV catalog for over two years
☒ EPSS	0.922 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Out-of-band / urgent Patch or fixed version identified**CISA required action:** Apply updates per vendor instructions.

Basis: CISA KEV required action

Affected and fixed versions · 63 more affected products on the NVD record

PACKAGE	AFFECTED	FIXED IN	SOURCE
proliant ml10 gen9 server firmware	5.0	no fixed version listed	NVD
simatic itp1000 firmware	< 9.1.41.3024	9.1.41.3024	NVD
simatic ipc847d firmware	< 9.1.41.3024	9.1.41.3024	NVD
simatic ipc847c firmware	< 6.2.61.3535	6.2.61.3535	NVD
simatic ipc827d firmware	< 9.1.41.3024	9.1.41.3024	NVD
simatic ipc827c firmware	< 6.2.61.3535	6.2.61.3535	NVD
simatic ipc677d firmware	< 9.1.41.3024	9.1.41.3024	NVD
simatic ipc677c firmware	< 6.2.61.3535	no fixed version listed	NVD

Sources

Vendor guidance	security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00075&languageid=en-fr	NVD	nvd.nist.gov/vuln/detail/CVE-2017-5689
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2017-14766
Current data	evulnable.com/vulnerability-management/cve/CVE-2017-5689		

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