CVE-2017-5689

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

Summary

CVE	CVE-2017-5689
State	PUBLISHED
Assigner	intel
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-05-02 14:59:00 UTC
Updated	2026-04-22 16:06:47 UTC
Description	An unprivileged network attacker could gain system privileges to provisioned Intel manageability SKUs: Intel Active Manage

Risk And Classification

Primary CVSS: v3.1 9.8 CRITICAL from nvd@nist.gov

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

EPSS: 0.941940000 probability, percentile 0.999220000 (date 2026-04-22)

CISA KEV: Listed on 2022-01-28; due 2022-07-28; ransomware use Unknown

Problem Types: NVD-CWE-noinfo | CWE-269 | Escalation of Privilege | CWE-269 CWE-269 Improper Privilege Management

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	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	ADP	DECLARED	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
2.0	nvd@nist.gov	Primary	10		AV:N/AC:L/Au:N/C:C/I:C/A:C

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

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

CISA Known Exploited Vulnerability

Vendor	Intel
Product	Active Management Technology (AMT), Small Business Technology (SBT), and Standard Manageability
Name	Intel Active Management Technology (AMT), Small Business Technology (SBT), and Standard Manageability Privilege Escalation Vulnerability
Required Action	Apply updates per vendor instructions.
Notes	https://nvd.nist.gov/vuln/detail/CVE-2017-5689

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Hpe	Proliant Ml10 Gen9 Server	-	All	All	All
Operating System	Hpe	Proliant Ml10 Gen9 Server Firmware	5.0	All	All	All
Hardware	Siemens	Simatic Field Pg M3	-	All	All	All
Operating System	Siemens	Simatic Field Pg M3 Firmware	All	All	All	All

Hardware	Siemens	Simatic Field Pg M4	-	All	All	All
Operating System	Siemens	Simatic Field Pg M4 Firmware	All	All	All	All
Hardware	Siemens	Simatic Field Pg M5	-	All	All	All
Operating System	Siemens	Simatic Field Pg M5 Firmware	All	All	All	All
Hardware	Siemens	Simatic Ipc477d	-	All	All	All
Operating System	Siemens	Simatic Ipc477d Firmware	-	All	All	All
Operating System	Siemens	Simatic Ipc477d Firmware	-	All	All	All
Hardware	Siemens	Simatic Ipc477e	-	All	All	All
Operating System	Siemens	Simatic Ipc477e Firmware	All	All	All	All
Hardware	Siemens	Simatic Ipc547d	-	All	All	All
Operating System	Siemens	Simatic Ipc547d Firmware	All	All	All	All
Hardware	Siemens	Simatic Ipc547e	-	All	All	All
Operating System	Siemens	Simatic Ipc547e Firmware	All	All	All	All
Hardware	Siemens	Simatic Ipc547g	-	All	All	All
Operating System	Siemens	Simatic Ipc547g Firmware	All	All	All	All
Hardware	Siemens	Simatic Ipc627c	-	All	All	All
Operating System	Siemens	Simatic Ipc627c Firmware	All	All	All	All
Hardware	Siemens	Simatic Ipc627d	-	All	All	All
Operating System	Siemens	Simatic Ipc627d Firmware	All	All	All	All
Hardware	Siemens	Simatic Ipc647c	-	All	All	All
Operating System	Siemens	Simatic Ipc647c Firmware	All	All	All	All
Hardware	Siemens	Simatic Ipc647d	-	All	All	All
Operating System	Siemens	Simatic Ipc647d Firmware	All	All	All	All
Hardware	Siemens	Simatic Ipc677c	-	All	All	All
Operating System	Siemens	Simatic Ipc677c Firmware	All	All	All	All
Hardware	Siemens	Simatic Ipc677d	-	All	All	All
Operating System	Siemens	Simatic Ipc677d Firmware	All	All	All	All
Hardware	Siemens	Simatic Ipc827c	-	All	All	All
Operating System	Siemens	Simatic Ipc827c Firmware	All	All	All	All
Hardware	Siemens	Simatic Ipc827d	-	All	All	All
Operating System	Siemens	Simatic Ipc827d Firmware	All	All	All	All
Hardware	Siemens	Simatic Ipc847c	-	All	All	All
Operating System	Siemens	Simatic Ipc847c Firmware	All	All	All	All
Hardware	Siemens	Simatic Ipc847d	-	All	All	All
Operating System	Siemens	Simatic Ipc847d Firmware	All	All	All	All
Hardware	Siemens	Simatic Itp1000	-	All	All	All

Operating System	Siemens	Simatic Itp1000 Firmware	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Intel Corporation	Intel Active Mangement Technology Intel Small Business Technology Intel Standard Manageability	affected fix

References

Reference	Source
Rediscovering the Intel AMT Vulnerability - Blog | Tenable™	af854a3
Intel® Product Security Center	af854a3
cert-portal.siemens.com/productcert/pdf/ssa-874235.pdf	af854a3
Multiple Intel Products CVE-2017-5689 Privilege Escalation Vulnerability	af854a3
CVE-2017-5689 Intel Management Engine Vulnerability in Multiple NetApp Products | NetApp Product Security	af854a3
www.cisa.gov/known-exploited-vulnerabilities-catalog	134c70
MythBusters: CVE-2017-5689 – Embedi	af854a3
Online Casino Harmony Central. 99 Free Spins & 200% Bonus!	af854a3
downloadmirror.intel.com/26754/eng/INTEL-SA-00075%20Mitigation%20Guide-Rev%201.1.pdf	af854a3
Intel Active Management Technology Authentication Flaw Lets Remote and Local Users Gain Elevated Privileges - SecurityTracker	af854a3
Oracle Critical Patch Update - July 2017	af854a3
HPE Support document - HPE Support Center	af854a3
CVE Program record	CVE.OR
NVD vulnerability detail	NVD
CISA Known Exploited Vulnerabilities catalog	CISA

No vendor comments have been submitted for this CVE.

Additional Advisory Data

Source	Time	Event
ADP	2022-01-28T00:00:00.000Z	CVE-2017-5689 added to CISA KEV

There are currently no legacy QID mappings associated with this CVE.

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred trademarks of The MITRE Corporation and the authoritative source of CVE content is MITRE's CVE web site. This site includes MITRE data granted under the following license.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report