CSAI Foundation

Cloud Security Alliance AI Safety Initiative

Four Critical CVEs in Cisco Webex and ISE

Full User Impersonation and 9.9-Severity RCE Demand Immediate Response

Unofficial AI-assisted Research

2026-04-17

Key Takeaways

- CVE-2026-20184 (CVSS 9.8) allows an unauthenticated remote attacker to impersonate any Webex user by exploiting a SAML certificate validation flaw in Cisco Webex's single sign-on integration; Cisco has patched the cloud service but organizations using SSO must manually upload a new IdP SAML certificate to Control Hub to fully close the vulnerability [1].
- Three additional critical flaws in Cisco Identity Services Engine — CVE-2026-20147, CVE-2026-20180, and CVE-2026-20186, all rated CVSS 9.9 — allow authenticated attackers to execute arbitrary commands on the ISE host operating system and escalate privileges to root via crafted HTTP requests [2][3].
- CVE-2026-20180 and CVE-2026-20186 are particularly concerning because they require only read-only administrative credentials to achieve full OS command execution, a privilege tier commonly provisioned for monitoring, compliance, and help-desk functions across a wider set of personnel than full admin access [3].
- Cisco ISE functions as the network access control policy enforcement point for enterprise wired, wireless, and VPN infrastructure; root-level compromise of an ISE node positions an attacker to inspect and manipulate network access policies for the entire attached network population [8].
- No workarounds are available for any of the ISE vulnerabilities; Cisco has released patches across active ISE release lines, and no active exploitation of any of the four CVEs has been confirmed as of the date of this note [2][3][6].

Background

Cisco Identity Services Engine: Network Access Control Policy Plane

Cisco Identity Services Engine is a centralized network access control platform that organizations deploy to enforce identity-based policies across enterprise network infrastructure. ISE acts as the combined policy decision point and enforcement point for controlling which users and devices are permitted to access which network segments, integrating across wired Ethernet switching, wireless LAN, VPN concentrators, and private 5G environments. The platform authenticates endpoints against Active

Directory and other identity stores, classifies devices by type and posture, and dynamically assigns them to VLANs and security groups based on contextual attributes including user role, device health, location, and time of day [8]. Cisco positions ISE as a foundational zero trust enforcement component for enterprise-scale network access control [8].

ISE Passive Identity Connector (ISE-PIC) is a companion product that extends passive identity collection to environments where full ISE policy enforcement is not deployed. Both ISE and ISE-PIC share the web-based administrative interface affected by the April 2026 vulnerabilities, and both are listed as impacted products in the relevant Cisco advisories [2].

The architecture of ISE means that a compromise of the platform is qualitatively different from a compromise of a standard application server. An attacker who gains root access to an ISE node occupies a position from which they can potentially read active session and policy databases, alter network access rules, reclassify endpoint devices into less-restricted security groups, and extract credential material used for integration with Active Directory, network switches, and wireless controllers. This scope of potential impact — spanning network access policy, endpoint classification, and credential stores — is broader than that of most application-layer vulnerabilities.

Cisco Webex: Enterprise Collaboration and SSO Federation

Cisco Webex is Cisco's unified enterprise collaboration platform, delivering video conferencing, messaging, calling, and team workspace capabilities to organizations worldwide. Like most enterprise SaaS platforms at scale, Webex supports SAML-based single sign-on federation, allowing organizations to authenticate Webex users through their existing identity providers. This integration is configured and managed through Cisco's Control Hub administrative console, which serves as the unified management plane for Webex collaboration, calling, and contact center services.

The SSO integration in Webex Control Hub relies on SAML certificates to establish cryptographic trust between the customer's identity provider and Cisco's cloud services. This trust relationship is the basis on which Webex determines whether to accept a SAML assertion as legitimate: the entire SSO chain is only as strong as the certificate validation logic governing that determination. CVE-2026-20184 compromises this foundation.

Security Analysis

The Four Critical CVEs at a Glance

CVE	CVSS	Product	Authentication Required	Primary Impact
CVE-2026-20184	9.8	Webex Services / Control Hub	None (unauthenticated)	Full user impersonation
CVE-2026-20147	9.9	Cisco ISE, ISE-PIC	Full admin credentials	RCE with root escalation
CVE-2026-20180	9.9	Cisco ISE	Read-only admin credentials	OS command execution, root escalation
CVE-2026-20186	9.9	Cisco ISE	Read-only admin credentials	OS command execution, root escalation

A companion medium-severity vulnerability, CVE-2026-20148 (CVSS 4.9), was disclosed in the same advisory as CVE-2026-20147 [2]. It enables authenticated administrators to conduct path traversal attacks that read arbitrary files from the ISE host operating system. While below the critical threshold, it extends the information disclosure surface on unpatched ISE nodes and is addressed by the same patch set as CVE-2026-20147.

CVE-2026-20184: Full Webex User Impersonation Without Credentials

CVE-2026-20184 is classified under CWE-295 (Improper Certificate Validation) and resides in the integration between Webex Services and the Control Hub SSO implementation [7]. When a user authenticates through an identity provider and receives a SAML assertion, Webex is expected to validate the cryptographic certificate associated with that assertion before accepting it as legitimate. The

vulnerability causes Webex to accept malformed or attacker-controlled SAML assertions, enabling an unauthenticated remote attacker to submit a crafted token and assume the identity of any user within the service without possessing that user's credentials [1][4][9].

The attack requires no prior authentication and no privileged network position — an attacker reachable to the Webex service endpoint is the only precondition, making the vulnerability accessible to a broad range of threat actors. The scope of the impersonation extends to all Webex services integrated with Control Hub, including collaboration, calling, and contact center workloads, allowing an attacker to access meeting content, communications, and organizational data associated with the impersonated account.

Cisco applied a server-side fix to the Webex cloud infrastructure, but this fix alone is insufficient for customers who have SSO integration configured. Those organizations must manually upload a new identity provider SAML certificate to Control Hub; without this update, the trust anchor remains in a vulnerable state even after the platform-side patch has been deployed [1][5]. The Control Hub Alerts center displays currently installed certificates and their validity status, and Cisco's integrated SSO wizard provides step-by-step guidance for certificate replacement.

CVE-2026-20147: ISE Remote Code Execution with Full Admin Credentials

CVE-2026-20147 carries a CVSS base score of 9.9 and affects both Cisco ISE and ISE-PIC [2]. The vulnerability stems from insufficient validation of user-supplied input processed via HTTP requests submitted to the ISE administrative interface. An attacker holding valid full administrative credentials can send specially crafted HTTP requests that the application passes to the underlying operating system without adequate sanitization, resulting in code execution at the operating system user level. From that foothold, the attacker can escalate privileges to root, achieving complete control over the affected ISE node [2][10].

Single-node ISE deployments face an additional consequence: Cisco's advisory notes that successful exploitation can render the ISE node unavailable, causing a denial-of-service condition that prevents endpoints which have not yet authenticated from accessing the network until the node is restored [2]. In distributed deployments, ISE failover may mitigate availability impact, but attacker access to a NAC enforcement host represents a significantly elevated risk regardless of deployment topology.

Cisco confirmed that no workarounds exist for this vulnerability and that software patching is the only available remediation [2].

CVE-2026-20180 and CVE-2026-20186: ISE Command Execution via Read-Only Admin Access

CVE-2026-20180 and CVE-2026-20186 share a CVSS base score of 9.9 and a CVSS vector of `CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H` [3]. Both vulnerabilities arise from the same root cause as CVE-2026-20147 — insufficient input validation in ISE's handling of crafted HTTP requests — but the code paths triggering them are reachable with read-only administrative credentials, representing a materially lower exploitation threshold.

The significance of this privilege differential warrants careful attention. In many enterprise deployments, read-only administrative accounts in ISE are provisioned for monitoring dashboards, compliance reporting, network operations center visibility, and help desk functions. Such accounts are often distributed to a broader set of users than full administrative roles, may be shared across teams, and are sometimes held by third-party managed service providers or auditing firms. An attacker who obtains read-only ISE credentials through phishing, credential stuffing, or access to a compromised monitoring system gains a path to full OS-level command execution and root escalation on the ISE host [3][11]. The practical implication is that the security perimeter protecting ISE against these two CVEs is substantially wider than the perimeter protecting it against CVE-2026-20147.

ISE version 3.5 is not affected by CVE-2026-20180 or CVE-2026-20186; all earlier supported releases require patching, and releases predating 3.2 must be migrated to a supported version before a patch can be applied [3].

Compounding Risk: Chaining and Lateral Movement Potential

While each of the four CVEs can be exploited independently, security teams should evaluate the chaining potential of the ISE vulnerabilities against the broader enterprise identity and access control estate. An attacker who compromises ISE at the OS level obtains access to the ISE policy database, which contains the full network access control rule set, security group assignments, and endpoint classifications for the enterprise network. The same host may hold Active Directory integration service accounts with broad directory read access, RADIUS shared secrets for authenticating network equipment, and API credentials for integration with network switches, wireless LAN controllers, and VPN gateways.

The Webex SSO vulnerability introduces a complementary vector: an attacker who successfully impersonates a Webex user may gain access to meeting recordings, shared files, and real-time communications that contain information useful for subsequent attacks — including credentials, architecture discussions, or incident response communications — without touching the network infrastructure at all.

Recommendations

Immediate Actions

Organizations using Webex with SSO integration should treat the SAML certificate update in Control Hub as a highest-priority remediation task. Cisco has completed the server-side fix, but customer action is mandatory and no workaround exists in the interim. Administrators should log into Control Hub, navigate to the SSO configuration, verify the certificate status through the Alerts center, and upload the new IdP SAML certificate using the SSO wizard before any other change management activity.

For ISE deployments, the highest-priority action is applying the appropriate software patch for each release line in production. The required patches by release are:

ISE Release	Patch for CVE-2026-20147 / CVE-2026-20148	Patch for CVE-2026-20180 / CVE-2026-20186
3.1	Patch 11	Migrate to 3.2 or later
3.2	Patch 10	Patch 8
3.3	Patch 11	Patch 8
3.4	Patch 6	Patch 4
3.5	Patch 3	Not vulnerable

Sources: Cisco Security Advisories [2][3]

Concurrently, administrators should audit all ISE accounts with administrative access — including read-only roles — and immediately rotate credentials for any account whose provenance, exposure, or access history cannot be confirmed. Given that read-only admin access is sufficient for two of the three ISE critical CVEs, the credential scope of concern extends well beyond the full-admin tier.

Short-Term Mitigations

Network access to the ISE administrative interface should be restricted to management network segments using firewall rules or infrastructure ACLs. Neither CVE-2026-20180 nor CVE-2026-20186 can be triggered without HTTP access to the ISE administrative interface, and reducing the network surface reachable to that interface limits the exposure window during the patching period.

Security teams should review read-only ISE administrative account provisioning practices and evaluate whether the breadth of access currently granted to monitoring tools, compliance auditors, and third-party managed service providers is consistent with the risk now confirmed by these vulnerabilities. Where read-only credentials have been shared with external parties or used in automated integrations, rotating those credentials should be treated as an immediate operational task regardless of patch status.

Organizations with single-node ISE deployments should assess whether temporary redundancy improvements are warranted during the patching window, particularly in environments where ISE availability is directly coupled to network access for a large number of endpoints. A DoS condition triggered by CVE-2026-20147 exploitation against a single-node deployment could deny network access to all unauthenticated endpoints until service is restored.

Enhanced logging and alerting for anomalous administrative activity in ISE and Webex Control Hub should be enabled across all affected deployments. While no active exploitation has been confirmed as of April 17, 2026 [2][3][6], observed patterns in vulnerability exploitation suggest that the window between public disclosure and weaponization is often measured in days rather than months; establishing detection baselines before exploit code becomes publicly available is materially more effective than retroactive investigation.

Strategic Considerations

These four CVEs are collectively a signal that network access control infrastructure and enterprise collaboration platforms have matured as attacker targets. ISE is not a general-purpose application — it is the network identity enforcement plane — and a vulnerability in it cannot be evaluated using the same risk calculus applied to a web application or a database server. Security teams should ensure that ISE patching cadence, change management urgency, and monitoring coverage match the platform's actual position in the enterprise architecture.

The read-only admin exploitation path in CVE-2026-20180 and CVE-2026-20186 specifically challenges a common assumption: that lower-privilege accounts represent an acceptable risk reduction in administrative access models. When a read-only account is sufficient to achieve root execution on a critical security control plane, the effective privilege boundary between read-only access and full OS

control has been eliminated by this vulnerability class. Organizations should revisit their ISE role definitions, evaluate whether read-only access genuinely requires network-level access to the administrative interface, and consider whether privileged access workstations and just-in-time access mechanisms should be applied to all ISE administrative roles, not only full administrators.

Certificate lifecycle tooling for SSO integrations varies widely across organizations, and those without automated inventory and alerting are more likely to miss time-sensitive remediation requirements like the SAML certificate update mandated by CVE-2026-20184. The manual remediation requirement — uploading a new SAML certificate to Control Hub — depends on administrators knowing that the action is required and completing it promptly. Organizations should invest in tooling that monitors SAML certificate validity and alerts on approaching expiry or required updates across all SSO integrations.

CSA Resource Alignment

MAESTRO: Agentic AI Threat Modeling

CSA's MAESTRO framework, which defines threat layers for AI systems and agentic architectures [12], provides relevant context for the Webex impersonation vulnerability. MAESTRO's threat model addresses identity spoofing, token forgery, and trust boundary violations as core threat categories for AI agents operating within enterprise SaaS environments [12]. As AI agents increasingly authenticate to collaboration platforms like Webex to retrieve meeting content, summarize communications, and act on behalf of users, the ability of an unauthenticated attacker to impersonate any Webex user becomes not only a credential theft risk but an agentic trust subversion risk. An AI agent that acts on Webex context it believes belongs to a legitimate user is potentially manipulable by an adversary who can inject attacker-controlled content into the impersonated account's workspace.

AI Controls Matrix and Zero Trust Guidance

CSA's AI Controls Matrix (AICM) — which extends the Cloud Controls Matrix to address AI-specific risk domains [13] — covers privileged access governance, credential management, and software patching cadence in the domains most directly relevant to these vulnerabilities. AICM controls covering identity verification, least-privilege access, and supply chain risk management apply directly to ISE administrative account governance and to the third-party access patterns that CVE-2026-20180 and CVE-2026-20186 exploit.

CSA's Zero Trust guidance is directly applicable to ISE because Cisco markets ISE as a zero trust enforcement component. The zero trust principle of verifying access continuously — including the integrity of the policy enforcement infrastructure itself — implies that ISE nodes should be subject to the same configuration assurance, vulnerability management, and anomaly detection standards as identity providers and network perimeter controls. Organizations that treat ISE as infrastructure rather than as a security control may apply less rigorous change management to it than the risk warrants.

STAR and Vendor Risk Management

The Security Trust Assurance and Risk (STAR) registry [14] and CSA's vendor risk management guidance are relevant for organizations that use managed ISE services or that grant ISE administrative access to third-party providers. The read-only admin exploitation path creates a direct vendor risk management consideration: if a managed service provider's staff or tooling hold ISE credentials, the organization's ISE deployment is exposed to the risk profile of that provider's credential management practices. STAR-aligned vendor assessments should include specific inquiry into which external parties hold ISE administrative access at any privilege level and what controls govern those credentials.

References

[1] Cisco Systems. "Cisco Webex Services Vulnerability (CVE-2026-20184)." Cisco Security Advisory cisco-sa-webex-cui-cert-8jSZYhWL, April 2026.

[2] Cisco Systems. "Cisco Identity Services Engine Remote Code Execution and Path Traversal Vulnerabilities." Cisco Security Advisory cisco-sa-ise-rce-traversal-8bYndVrZ, April 2026.

[3] Cisco Systems. "Cisco Identity Services Engine Remote Code Execution Vulnerabilities." Cisco Security Advisory cisco-sa-ise-rce-4fverepv, April 2026.

[4] The Hacker News. "Cisco Patches Four Critical Identity Services, Webex Flaws Enabling Code Execution." The Hacker News, April 16, 2026.

[5] BleepingComputer. "Cisco Says Critical Webex Services Flaw Requires Customer Action." BleepingComputer, April 2026.

[6] Cyber Security Agency of Singapore. "Critical Vulnerabilities in Cisco ISE and Webex Services." CSA Singapore Alert AL-2026-040, April 17, 2026.

[7] CSO Online. "Cisco Webex SSO flaw needs manual certificate update to fix." CSO Online, April 2026.

[8] Cisco Systems. "Cisco Identity Services Engine — Product Overview." Cisco, 2026.

[9] Cybersecurity News. "Cisco Webex Services Vulnerability Let Remote Attacker Impersonate Any User." Cybersecurity News, April 2026.

[10] Cybersecurity News. "Critical Cisco ISE Vulnerabilities Let Remote Attackers Execute Malicious Code." Cybersecurity News, April 2026.

[11] Security Affairs. "Cisco Fixed Four Critical Flaws in Identity Services and Webex." Security Affairs, April 2026.

[12] Cloud Security Alliance. "Agentic AI Threat Modeling Framework: MAESTRO." CSA AI Safety Initiative, February 2025.

[13] Cloud Security Alliance. "AI Controls Matrix." CSA, 2025.

[14] Cloud Security Alliance. "CSA STAR for AI." CSA, 2026.