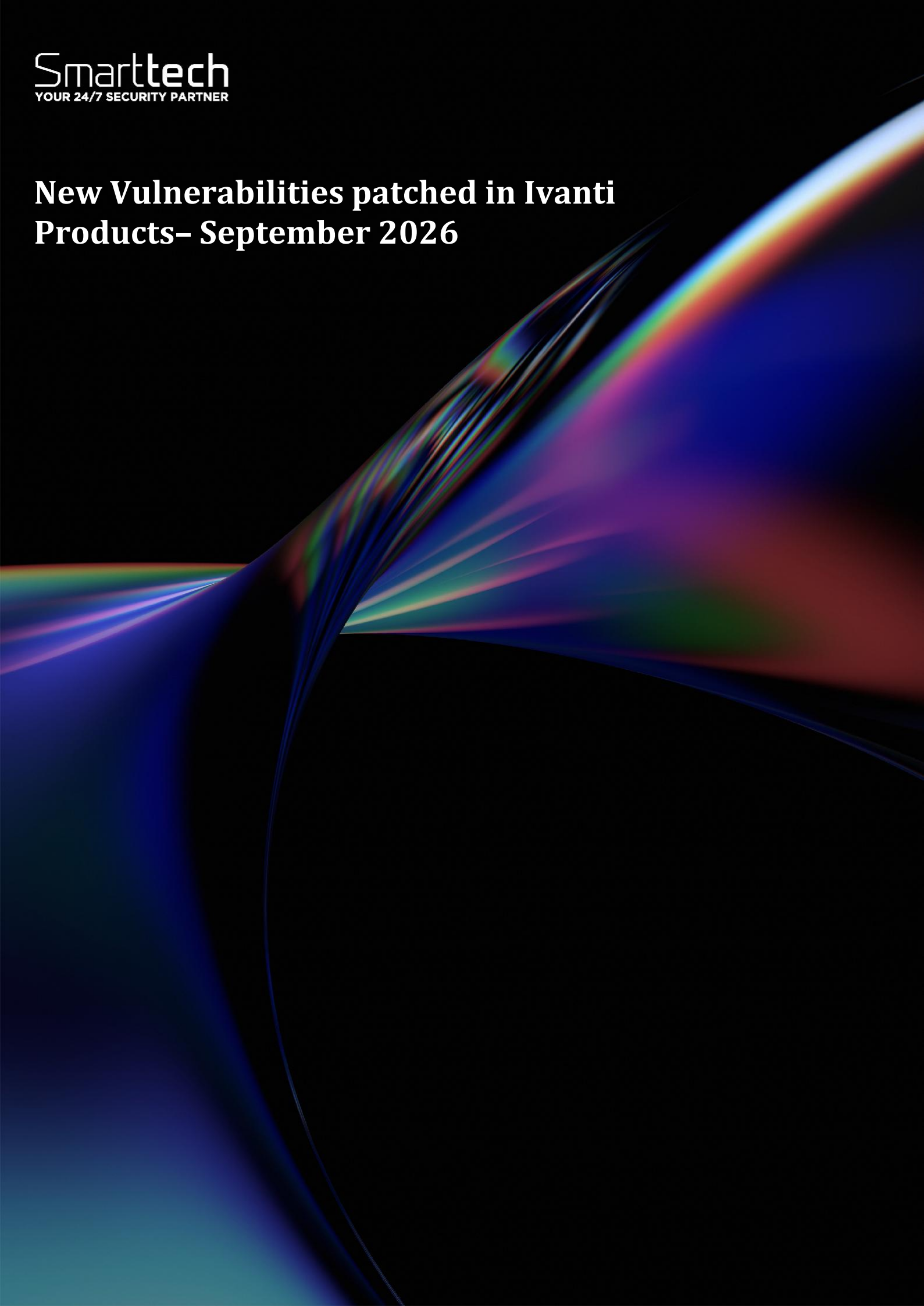
Smarttech
YOUR 24/7 SECURITY PARTNER

New Vulnerabilities patched in Ivanti Products– September 2026



Document ID	SMA-Threat Report
Document status	ISSUED
Issue Number	155
Authors	Daniel-Cristian Carp < daniel.carp@smarttech247.com >
Verified by	Alin Curcan < alin.curcan@smarttech247.com >
Last modified	2026-09-09
Issue Date	2026-09-09

Threat Reports are reports created by Smarttech247 based on high and critical severity vulnerabilities that may have a high potential to be exploited in the wild i.e. vulnerabilities that are present in most used products by companies and do not have an auto-update option or they are usually not automatically updated in case that could lead to some service disruption. This report is usually created as soon as the vulnerability is released, therefore we strongly recommend that the information is reviewed, tests are performed and patches are applied before the first proof-of-concept is released.
Even though certain vulnerabilities may not have an active exploit in the wild at the time that we report on them, we take into consideration the wider risk and the impact it could have on systems, should an exploit like that be available after a while. Our duty is to report them on time and we recommend enterprises that, in order to keep critical business systems protected, they should consider, on average, ten working days to check whether or not the new vulnerability affects them, and if so, to implement actions in order to remove the risk.

Overview

Multiple vulnerabilities have been identified across the following Ivanti products: Ivanti Neurons for ITSM, Ivanti Endpoint Manager Mobile and Ivanti Sentry. The discovered issues range from deserialization of untrusted data and missing authorization to authentication bypass vulnerabilities, potentially allowing remote attackers to execute arbitrary code, escalate privileges, or gain administrative-level access.

RISK

Government:

- Large and medium government entities: **High**
- Small government entities: **Medium**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **Medium**

TECHNICAL SUMMARY

The following table summarizes the identified vulnerabilities, including their CVE identifiers, CVSS severity scores, and technical descriptions. If successfully exploited, these vulnerabilities could allow remote unauthenticated or authenticated attackers to execute arbitrary code, bypass authentication, escalate privileges to administrative levels, and gain unauthorized access to affected systems. Several of the affected products are commonly deployed in enterprise environments and may expose critical infrastructure components to compromise if left unpatched.

CVE ID	***Description***
CVE-2026-12744 **CVSS Score: 9.8**	A Deserialization of Untrusted Data vulnerability in Ivanti Neurons for ITSM before 2026.2 allows a remote unauthenticated attacker to execute arbitrary code on the server.
CVE-2026-12745 **CVSS Score: 9.8**	A Deserialization of Untrusted Data vulnerability in Ivanti Neurons for ITSM before 2026.2 allows a remote unauthenticated attacker to execute arbitrary code on the server.
CVE-2026-12651 **CVSS Score: 8.8**	A Deserialization of Untrusted Data vulnerability in Ivanti Neurons for ITSM before 2026.2 allows a remote authenticated attacker to execute arbitrary code on the server.

CVE-2026-12650 **CVSS Score: 9.9**	A Deserialization of Untrusted Data vulnerability in Ivanti Neurons for ITSM before 2026.2 allows a remote authenticated attacker to execute arbitrary code on the server.
CVE-2026-12648 **CVSS Score: 8.8**	A Deserialization of Untrusted Data vulnerability in Ivanti Neurons for ITSM before 2026.2 allows a remote authenticated attacker to execute arbitrary code on the server.
CVE-2026-12645 **CVSS Score: 9.9**	A Missing Authorization vulnerability in Ivanti Neurons for ITSM before 2026.2 allows a remote authenticated attacker to execute arbitrary code on the server.
CVE-2026-12646 **CVSS Score: 9.9**	A Missing Authorization vulnerability in Ivanti Neurons for ITSM before 2026.2 allows a remote authenticated attacker to execute arbitrary code on the server.
CVE-2026-12647 **CVSS Score: 9.9**	A Missing Authorization vulnerability in Ivanti Neurons for ITSM before 2026.2 allows a remote authenticated attacker to execute arbitrary code on the server.
CVE-2026-18851 **CVSS Score: 8.8**	Missing authorization in Ivanti Endpoint Manager Mobile before version 12.10.0.0, 12.9.0.2, and 12.8.0.4 allows a remote authenticated attacker to escalate their privileges to admin.
CVE-2026-83527 **CVSS Score: 8.1**	An Authentication Bypass vulnerability in Sentry before R10.8.2, R10.7.3 and R10.6.4 allows a remote unauthenticated attacker to gain administrative level access.

Affected Versions

Product Name	Affected Version(s)	Resolved Version(s)	Patch Availability
Ivanti Neurons for ITSM (Cloud / SaaS)	2026.2	mo2026.2	The fix was applied to all cloud landscapes on August 9, 2026
Ivanti Neurons for ITSM On-Prem	2025.2, 2025.3, 2025.4, 2026.1	2025.2 Sept 2026 Security Patch, 2025.3 Sept 2026 Security Patch, 2025.4 Sept 2026 Security Patch, 2026.1 Sept 2026 Security Patch, 2026.2	Download Available in ILS
Ivanti Endpoint Manager Mobile (EPMM)	12.9.0.1 and prior 12.8.0.3 and prior	12.10.0.0 12.9.0.2 12.8.0.4	Customers can access the applicable patch links through the Ivanti Security Advisory page. Login required.
Ivanti Sentry	R10.8.1 and prior R10.7.2 and prior R10.6.3 and prior	R10.8.2 R10.7.3 R10.6.4	Customers can access the applicable patch links through the Ivanti Security Advisory page. Login required.

Recommendations

Smarttech247 team **highly** recommends the following actions be taken:

- Apply appropriate updates provided by Ivanti to vulnerable systems immediately after appropriate testing. (**M1051: Update Software**)
    - **Safeguard 7.1 : Establish and Maintain a Vulnerability Management Process:** Establish and maintain a documented vulnerability management process for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.
    - **Safeguard 7.2: Establish and Maintain a Remediation Process:** Establish and maintain a risk-based remediation strategy documented in a remediation process, with monthly, or more frequent, reviews.
    - **Safeguard 7.4: Perform Automated Application Patch Management:** Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.
    - **Safeguard 7.5 : Perform Automated Vulnerability Scans of Internal Enterprise Assets:** Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.
    - **Safeguard 7.7: Remediate Detected Vulnerabilities:** Remediate detected vulnerabilities in software through processes and tooling on a monthly, or more frequent, basis, based on the remediation process.
    - **Safeguard 12.1: Ensure Network Infrastructure is Up-to-Date:** Ensure network infrastructure is kept up-to-date. Example implementations include running the latest stable release of software and/or using currently supported network-as-a-service (NaaS) offerings. Review software versions monthly, or more frequently, to verify software support.
    - **Safeguard 18.1: Establish and Maintain a Penetration Testing Program:** Establish and maintain a penetration testing program appropriate to the size, complexity, and maturity of the enterprise. Penetration testing program characteristics include scope, such as network, web application, Application Programming Interface (API), hosted services, and physical premise controls; frequency; limitations, such as acceptable hours, and excluded attack types; point of contact information; remediation, such as how findings will be routed internally; and retrospective requirements.
    - **Safeguard 18.2: Perform Periodic External Penetration Tests:** Perform periodic external penetration tests based on program requirements, no less than annually. External penetration testing must include enterprise and environmental reconnaissance to detect exploitable information. Penetration testing requires specialized skills and experience and must be conducted through a qualified party. The testing may be clear box or opaque box.
    - **Safeguard 18.3: Remediate Penetration Test Findings:** Remediate penetration test findings based on the enterprise's policy for remediation scope and prioritization.
- Apply the Principle of Least Privilege to all systems and services. Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack. (**M1026: Privileged Account Management**)

    - **Safeguard 4.7: Manage Default Accounts on Enterprise Assets and Software:** Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.
    - **Safeguard 5.5: Establish and Maintain an Inventory of Service Accounts:** Establish and maintain an inventory of service accounts. The inventory, at a minimum, must contain department owner, review date, and purpose. Perform service account reviews to validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.
- Vulnerability scanning is used to find potentially exploitable software vulnerabilities to remediate them. (**M1016**: **Vulnerability Scanning**)
    - **Safeguard 16.13: Conduct Application Penetration Testing:** Conduct application penetration testing. For critical applications, authenticated penetration testing is better suited to finding business logic vulnerabilities than code scanning and automated security testing. Penetration testing relies on the skill of the tester to manually manipulate an application as an authenticated and unauthenticated user.
- Architect sections of the network to isolate critical systems, functions, or resources. Use physical and logical segmentation to prevent access to potentially sensitive systems and information. Use a DMZ to contain any internet-facing services that should not be exposed from the internal network. Configure separate virtual private cloud (VPC) instances to isolate critical cloud systems. (**M1030**: **Network Segmentation**)
    - **Safeguard 12.2: Establish and Maintain a Secure Network Architecture:** Establish and maintain a secure network architecture. A secure network architecture must address segmentation, least privilege, and availability, at a minimum.
- Use capabilities to detect and block conditions that may lead to or be indicative of a software exploit occurring. (**M1050**: **Exploit Protection**)
    - **Safeguard 10.5: Enable Anti-Exploitation Features:** Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft? Data Execution Prevention (DEP), Windows? Defender Exploit Guard (WDEG), or Apple? System Integrity Protection (SIP) and Gatekeeper™.

References

IVANTI

September 2026 Security Update | Ivanti
Security Advisory Ivanti Neurons for ITSM (Multiple CVEs)
Security Advisory - Ivanti Endpoint Manager Mobile (CVE-2026-18851)
Security Advisory Ivanti Sentry (CVE-2026-83527)

CVEs

- **CVE-2026-12744**
- **CVE-2026-12745**
- **CVE-2026-12651**
- **CVE-2026-12650**
- **CVE-2026-12648**

- CVE-2026-12645
- CVE-2026-12646
- CVE-2026-12647
- CVE-2026-18851
- CVE-2026-83527

Smarttech
YOUR 24/7 SECURITY PARTNER

www.smarttech247.com