

// PUBLIC • SOURCE-LEVEL AUDIT

# Security Audit.

## Lenovo notebook BIOS, SMM handler validation

|                |                                                 |
|----------------|-------------------------------------------------|
| TARGET         | Lenovo Legion 5 15IRX10 (83LY), Insyde H2O BIOS |
| BUILD          | BIOS QNCN33WW (v1.33)                           |
| DATE           | September 2026                                  |
| PREPARED BY    | Eva Crystal (Oxiviél), XSource Security         |
| CLASSIFICATION | Public                                          |

# Executive summary

XSource Security audited the System Management Mode handler surface of the Lenovo Legion 5 15IRX10 notebook at BIOS build QNCN33WW (v1.33, Insyde H2O). The review was a binary-level firmware analysis, self-funded, and the results were disclosed to Lenovo PSIRT under coordinated disclosure with a 90-day window.

Six findings were reported. Four were confirmed and are now public as CVE-2026-10587, CVE-2026-10588, CVE-2026-10589 and CVE-2026-10590, all fixed and credited. One was routed to the component owner. One was not accepted. All four confirmed findings sit in the same BIOS customization module and concern its handling of input from the operating system into System Management Mode.

Lenovo published advisory LEN-220440 on 2026-07-14, titled "Multi-Vendor BIOS Security Vulnerabilities (July 2026)". The advisory covers findings from multiple reporters and carries an overall severity of High with industry-wide scope of impact. The four findings in this report are each rated Medium individually by the CNA. The advisory has been revised ten times, most recently on 2026-09-03, all updating product impact.

|                              |                               |
|------------------------------|-------------------------------|
| Findings reported            | 6                             |
| Findings confirmed           | 4                             |
| Highest severity             | 6.0 Medium (CVSS 3.1, Lenovo) |
| Advisory severity            | High (LEN-220440, overall)    |
| Time from report to advisory | 128 days                      |
| Status                       | Published, fixed              |

# Methodology

The review followed the standard XSource audit method, adapted for a closed-source firmware target:

- **Binary analysis of extracted firmware.** The BIOS SPI flash was read from the audited system, firmware volumes were extracted, and the Lenovo-specific SMM handler modules were disassembled and analysed statically. No vendor source code was available or used.
- **Trust boundaries before bug classes.** The surface was mapped by where OS-level input crosses into System Management Mode, not by scanning for known patterns. The four findings all sit at that boundary.

- **Reproduced, not inferred.** Each finding was demonstrated with a proof of concept against the audited BIOS build. The PoCs triggered the vulnerable paths from the operating system and confirmed the impact described in each finding.
- **Platform hardening assessed.** The audit included a full platform security configuration check covering Boot Guard, SMRR, SPI write protection, debug interface lock, manufacturing mode, and CPU microarchitectural mitigations. All were correctly configured and locked on the audited build.
- **Limits stated upfront.** What was not measured is named in the findings rather than left implicit. The PoCs and binary analysis detail are withheld from this public report; the mechanism of each finding is described at the level of the published CVE descriptions and the researcher's own blog series.

# Findings

| ID  | FINDING                                                          | SEVERITY                      | STATUS                |
|-----|------------------------------------------------------------------|-------------------------------|-----------------------|
| F01 | Out-of-bounds write in SMM handler via missing buffer validation | 6.0 Medium (CVSS 3.1, Lenovo) | Fixed, CVE-2026-10587 |
| F02 | SMM memory address disclosed through ACPI interface              | 4.4 Medium (CVSS 3.1, Lenovo) | Fixed, CVE-2026-10588 |
| F03 | Out-of-bounds write in SMM handler via missing size validation   | 6.0 Medium (CVSS 3.1, Lenovo) | Fixed, CVE-2026-10589 |
| F04 | BIOS configuration handler missing caller authentication         | 4.4 Medium (CVSS 3.1, Lenovo) | Fixed, CVE-2026-10590 |

---

## F01 • Out-of-bounds write in SMM handler via missing buffer validation

**Severity.** 6.0 Medium (CVSS 3.1, Lenovo). Vector `CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:H`. CVSS 4.0: 6.8 Medium (Lenovo), vector `CVSS:4.0/AV:L/AC:L/AT:N/PR:H/UI:N/VC:N/VI:H/VA:H/SC:N/SI:N/SA:N`. CWE-787, Out-of-bounds Write.

**Affected.** Lenovo notebook models listed in advisory LEN-220440. For the audited model, Legion 5 15IRX10 (83LY), BIOS builds before QNCN38WW are affected per the advisory (revision 10, 2026-09-03). The CVE record lists 57 affected models.

**Preconditions.** Local access with elevated privileges (ring-0). The attacker must be able to trigger the software SMI from the operating system.

### Root cause

The BIOS customization module's SMM handler does not call the standard UEFI buffer validation API before processing OS-supplied input. Data from an ACPI operation region is read directly into SMM without verifying that the source buffer lies outside SMRAM. This allows a local attacker with kernel-level access to write out of bounds, modifying power management settings and potentially other BIOS configuration stored in the handler's internal data structures.

### Reachability

The handler is reached by triggering a software SMI from the operating system through the standard ACPI WMI interface. The trigger path was confirmed on the audited build.

### Evidence

A proof of concept was developed and executed against BIOS QNCN33WW on the audited system. The PoC triggered the software SMI from the operating system and demonstrated the out-of-bounds write by modifying BIOS setup values that should not be writable from the OS. The PoC detail is withheld from this public report.

### Impact

Out-of-bounds write from ring-0 into SMM-managed BIOS configuration. The published CVE description states this allows modifying power management settings through an out-of-bounds write. The local finding confirmed modification of BIOS setup values including power management, PCIe configuration, and other platform settings through the unvalidated path.

### Stated limits

- The attack requires ring-0 (kernel-level) access on the target system. No remote or user-level path was shown.

- The CVSS 3.1 vector scores Scope as Unchanged (S:U). The local analysis estimates scope change is applicable, since the write crosses from ring-0 into SMM, but this report uses the CNA-assigned scores.
- The CVE records list the affected ceiling for the audited model as QNCN28WW. The advisory, revised ten times since initial publication, gives QNCN38WW as the minimum fix version. This report follows the advisory as the more current source; the CVE record version data has not been updated.

Remediation

Fixed by Lenovo in a BIOS update. For the audited model, the minimum fixed version is QNCN38WW per advisory LEN-220440.

Resolution

| DATE       | EVENT                                                                                                 |
|------------|-------------------------------------------------------------------------------------------------------|
| 2026-03-08 | Reported to Lenovo PSIRT with a proof of concept and full binary analysis                             |
| 2026-03-11 | Acknowledged by Lenovo PSIRT, tracked as LEN-213632, 90-day coordinated disclosure window established |
| 2026-03-13 | Initial assessment: four findings confirmed, one rejected, one routed to the component owner          |
| 2026-04-17 | Fixed BIOS packages expected end of June, advisory planned for Patch Tuesday in July                  |
| 2026-06-02 | CVEs reserved: CVE-2026-10587 through CVE-2026-10590                                                  |
| 2026-07-14 | Advisory LEN-220440 published, embargo lifted                                                         |
| 2026-07-18 | XSource Security blog series published                                                                |

Credit, verbatim from the advisory: "Lenovo thanks 0xiviell/Eva Crystal (XSource Security) for reporting CVE-2026-10587, CVE-2026-10588, CVE-2026-10589 and CVE-2026-10590."

---

## F02 • SMM memory address disclosed through ACPI interface

**Severity.** 4.4 Medium (CVSS 3.1, Lenovo). Vector `CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N`. CVSS 4.0: 6.7 Medium (Lenovo), vector

`CVSS:4.0/AV:L/AC:L/AT:N/PR:H/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N`. CWE-497, Exposure of Sensitive System Information to an Unauthorized Control Sphere.

**Affected.** Lenovo notebook models listed in advisory LEN-220440. For the audited model, BIOS builds before QNCN38WW. The CVE record lists 56 affected models.

**Preconditions.** Local access with elevated privileges (ring-0). The leaked address is readable from the operating system through a mapped ACPI region.

### Root cause

During initialisation, the same BIOS customization module writes an SMM-allocated buffer pointer into an ACPI operation region. Because the ACPI region is mapped into OS-accessible memory, the SMM buffer address is readable from ring-0. This discloses the layout of memory that should be protected by SMRAM access controls.

### Reachability

The information leak is passive: the address is written at boot and remains readable for the lifetime of the system. No SMI trigger is required. The disclosure was confirmed by reading the ACPI region from the operating system on the audited build.

### Evidence

Demonstrated on BIOS QNCN33WW. The SMM buffer address was read from the operating system without triggering any SMI, confirming the information is exposed at boot and persists.

### Impact

Disclosure of SMM memory layout to a ring-0 attacker. This is an information leak, not a write primitive, but it reduces the difficulty of exploiting any SMM vulnerability that requires knowledge of SMRAM addresses. It is complementary to F01 and F03.

### Stated limits

- Information disclosure only: no integrity or availability impact.
- The version discrepancy noted in F01 Stated limits applies to all four findings.

## **Remediation**

Fixed by Lenovo in a BIOS update. Minimum fixed version for the audited model: QNCN38WW per advisory LEN-220440.

## **Resolution**

All four findings share the same disclosure timeline; see F01 Resolution above.

---

## F03 • Out-of-bounds write in SMM handler via missing size validation

**Severity.** 6.0 Medium (CVSS 3.1, Lenovo). Vector `CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:H`. CVSS 4.0: 6.8 Medium (Lenovo), vector `CVSS:4.0/AV:L/AC:L/AT:N/PR:H/UI:N/VC:N/VI:H/VA:H/SC:N/SI:N/SA:N`. CWE-787, Out-of-bounds Write.

**Affected.** Lenovo notebook models listed in advisory LEN-220440. For the audited model, BIOS builds before QNCN38WW. The CVE record lists 56 affected models.

**Preconditions.** Local access with elevated privileges (ring-0). The attacker must be able to trigger the software SMI from the operating system.

### Root cause

The same BIOS customization module's SMM handler ignores the communication buffer size parameter entirely. The handler reads from an internal ACPI buffer without validating its bounds against the declared size, allowing an out-of-bounds write. This is a distinct defect from F01: F01 concerns the source buffer identity (missing SMRAM validation), while F03 concerns the source buffer bounds (missing size validation).

### Reachability

Same trigger path as F01: a software SMI through the ACPI WMI interface. Confirmed on the audited build.

### Evidence

A proof of concept was developed and executed against BIOS QNCN33WW, demonstrating that the handler processes input without checking the communication buffer size parameter. The PoC detail is withheld from this public report.

### Impact

Out-of-bounds write from ring-0 into SMM, potentially leading to arbitrary code execution in System Management Mode. The published CVE description describes this as allowing a local attacker with elevated privileges to execute arbitrary code through an out-of-bounds write.

### Stated limits

- Same privilege requirement as F01: ring-0 access.
- A mitigating factor exists: the internal buffer used by the handler is SMM-allocated and of fixed size, which constrains the reachable write window. The PoC demonstrated the out-of-bounds condition within those constraints.
- The version discrepancy noted in F01 Stated limits applies to all four findings.

## **Remediation**

Fixed by Lenovo in a BIOS update. Minimum fixed version for the audited model: QNCN38WW per advisory LEN-220440.

## **Resolution**

All four findings share the same disclosure timeline; see F01 Resolution above.

---

## F04 • BIOS configuration handler missing caller authentication

**Severity.** 4.4 Medium (CVSS 3.1, Lenovo). Vector `CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:N`. CVSS 4.0: 6.7 Medium (Lenovo), vector `CVSS:4.0/AV:L/AC:L/AT:N/PR:H/UI:N/VC:N/VI:H/VA:N/SC:N/SI:N/SA:N`. CWE-306, Missing Authentication for Critical Function.

**Affected.** Lenovo notebook models listed in advisory LEN-220440. For the audited model, BIOS builds before QNCN38WW. The CVE record lists 57 affected models.

**Preconditions.** Local access with elevated privileges (ring-0).

### Root cause

The BIOS customization module accepts WMI commands that modify firmware settings without authenticating the caller. Any ring-0 code that can trigger the software SMI through the ACPI WMI interface can change BIOS configuration, bypassing the intended restriction that these settings are managed only through the vendor's own interface.

### Reachability

Same trigger path as F01 and F03. The WMI interface is the standard path by which the vendor's own tools modify BIOS settings; the finding is that no authentication distinguishes the vendor's tools from arbitrary ring-0 code.

### Evidence

Demonstrated on BIOS QNCN33WW. The PoC modified BIOS configuration settings through the WMI interface without any authentication exchange. The PoC detail is withheld from this public report.

### Impact

Firmware settings modification from ring-0 without authorisation. An attacker with kernel-level access can change BIOS configuration through the same interface the vendor's own management tools use, with no credential or token required.

### Stated limits

- Integrity impact only: no confidentiality or availability impact per the CNA scoring.
- The version discrepancy noted in F01 Stated limits applies to all four findings.

## Remediation

Fixed by Lenovo in a BIOS update. Minimum fixed version for the audited model: QNCN38WW per advisory LEN-220440.

## Resolution

All four findings share the same disclosure timeline; see F01 Resolution above.

## Coverage

The following areas were examined within the scope of the audit. Areas that produced no finding are listed alongside those that did, because coverage and its limits are both part of what an audit delivers.

| AREA                                  | EXAMINED | RESULT                                                                                                                 |
|---------------------------------------|----------|------------------------------------------------------------------------------------------------------------------------|
| SMM handler buffer validation         | Yes      | F01 (CVE-2026-10587): out-of-bounds write via missing SMRAM buffer validation                                          |
| SMM address information exposure      | Yes      | F02 (CVE-2026-10588): SMM memory address leaked through ACPI operation region                                          |
| SMM handler size validation           | Yes      | F03 (CVE-2026-10589): out-of-bounds write via missing communication buffer size check                                  |
| SMM handler caller authentication     | Yes      | F04 (CVE-2026-10590): BIOS configuration commands accepted without authentication                                      |
| Additional finding reported to vendor | Yes      | Reported, routed to the component owner                                                                                |
| Additional finding reported to vendor | Yes      | Reported, not accepted                                                                                                 |
| Boot Guard configuration              | Yes      | Verified Boot and Measured Boot active, locked by field-programmable fuses                                             |
| SMRR and SMRAM protection             | Yes      | Valid on all logical processors, SMM_Code_Chk enabled and locked                                                       |
| SPI flash write protection            | Yes      | BIOS Lock Enable, SMM BIOS Write Protect, BIOS Interface Lock Down, and flash descriptor protection all set and locked |
| CSME firmware                         | Yes      | No novel vulnerability identified; firmware version outdated relative to published advisories                          |

| AREA                               | EXAMINED | RESULT                                                                                       |
|------------------------------------|----------|----------------------------------------------------------------------------------------------|
| Debug and manufacturing interfaces | Yes      | Debug interface disabled and locked, manufacturing mode off                                  |
| CPU microarchitectural mitigations | Yes      | All published mitigations active on all logical processors                                   |
| Additional SMM handler modules     | Yes      | Three additional Lenovo-specific SMM modules read; no finding meeting the reporting standard |

## Conclusion

All four findings sit in the same BIOS customization module and concern the same trust boundary: input arriving from the operating system through the ACPI WMI interface into System Management Mode. Three are buffer validation failures and one is missing authentication. The defect class is well known in UEFI firmware, with prior CVEs in the same and related vendors, and the standard mitigation APIs exist in the platform. The four findings are that those APIs were not called.

The platform is otherwise well hardened. Every Intel-mandated security mechanism checked during the audit, from Boot Guard through SMRR to SPI write protection, was correctly configured and locked. The findings are OEM BIOS implementation issues, not silicon defects.

Lenovo accepted the report, reserved CVEs within 86 days, published advisory LEN-220440 at 128 days, and credited the researcher. The coordinated disclosure window was respected by both sides.

## Appendix A • Reporting standard

Five conditions every XSource finding meets before it is written up:

- **Reproduced, not inferred.** Triggered against the agreed target in the agreed environment, or, where static analysis is the agreed method, reproduced as a standalone proof with the limits stated.
- **Reachable from a real position.** The attacker position is named and was actually held, or, where static analysis is the agreed method, the path to it is traced from source end to end with the limits stated.
- **Impact shown, not asserted.** Which data, whose data, or which action, with the evidence attached.
- **Checked against design and backlog first.** Anything that might be intended behaviour, or already tracked, is raised before it is written up as a defect.
- **Fixable as written.** Remediation names the location and the change, and says so plainly where the fix is a design decision rather than a patch.

