Analysis · Cybersecurity · 27 June 2026, 11:11 am IST · 18 min read · AUMAstra Security Intelligence
51 reads

Administrator Is Not Root: Inside a Critical Infoblox NIOS Privilege Escalation

AN AUMASTRA SECURITY INTELLIGENCE TECHNICAL ANALYSIS

How a Maintenance Mode trust-boundary failure led to appliance root, why the coordinated severity moved to CVSS 9.1 Critical, and what the disclosure process teaches product-security teams.

By AUMAstra Security Intelligence Published 27 June 2026, 11:11 am IST

UPDATED 8 OCTOBER 2026

CVE-2026-107510 published

Infoblox has published CVE-2026-107510 with a CVSS v3.1 score of 9.1 Critical. NVD lists the record as Received; independent NVD scoring is pending. The original June analysis remains preserved as a historical record.

Read the latest update and current standing



Security appliances are built around controlled authority. An administrator may configure DNS, DHCP, IP address management, diagnostics, backups and high-availability operations, but that authority is expected to remain inside the product's supported control plane.

A supported maintenance function that crosses from a constrained product interface into an unrestricted operating-system root shell changes that security model. It is not simply an administrator receiving one more administrative capability. It is a transition into a different security authority.

> **A product administrator is not automatically entitled to operating-system root.**

On 15 March 2026, AUMAstra Security Intelligence reported a privilege-escalation vulnerability in Infoblox NIOS. The issue allowed an authenticated user with access to the Maintenance Mode command-line interface to move beyond the intended NIOS administrative boundary and obtain root access to the underlying appliance operating system.

Infoblox validated the finding. After technical discussion, the parties agreed on a CVSS v3.1 score of **9.1 Critical**. Infoblox later reported hotfix availability for supported affected releases and stated that a permanent fix was included in NIOS 9.2.0. A revised advisory dated 24 June 2026 documented the Critical severity, agreed vector, CWE classifications and AUMLayer's research credit.

That remediation work matters. So do the remaining questions around public advisory accessibility, the final CVE identifier, precise affected-version wording and independent retesting of the complete exploit chain.



ATTRIBUTE	DETAIL
Vendor	Infoblox
Product	NIOS
Vulnerability	Maintenance Mode CLI privilege escalation to root
Validated build	NIOS 9.0.3 build 50212
Vendor-listed affected releases	NIOS 9.0.3 through 9.1.0
Vendor-reported remediation	Hotfixes for supported releases; permanent fix in NIOS 9.2.0
Internal fix reference	NIOS-109699
Final severity	Critical
Final CVSS v3.1	9.1
Final vector	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H
Primary weakness	CWE-88, argument injection
Related weaknesses	CWE-284, improper access control; CWE-269, improper privilege management
CVE status	No CVE ID shared with AUMLayer as of 23 June 2026

Summary of the validated finding, coordinated severity, CVSS vector and disclosure status as of 26 June 2026.
View full-resolution image ↗

At a glance

- The finding requires authenticated access to the NIOS Maintenance Mode CLI. It is not an unauthenticated remote exploit.

- Successful exploitation crosses from a supported product-administration interface into appliance operating-system root.
- The coordinated final severity is **CVSS 9.1 Critical**.
- Infoblox reports that hotfixes are available for supported affected releases and that NIOS 9.2.0 contains the permanent fix.
- AUMAstra had not independently retested the complete remediation chain as of 26 June 2026.
- Public CVE assignment, public advisory discoverability and affected-version reconciliation remained open at the status date.



Current technical, remediation and disclosure status as of 26 June 2026.
View full-resolution image ↗

The trust boundary that failed

The vulnerability arose from two weaknesses interacting across a privileged maintenance workflow.

1. User-controlled data crossed into a privileged component

An authenticated Maintenance Mode user could invoke a traffic-capture capability and provide a filter expression. The expected security property was simple: the value should remain data used to describe traffic.

Instead, the value reached a privileged downstream packet-capture component without sufficient separation between data and command options. Specially formed input could affect how the downstream utility interpreted the request.

At a weakness-class level, this is consistent with **CWE-88: Argument Injection or Modification**. The operational syntax is intentionally omitted.

2. A security-sensitive state transition could be influenced

The privileged behaviour could be used to satisfy a local condition associated with enabling a diagnostic shell. That shell-control design relied on local state without sufficiently strong verification of who created the state, how it was created and whether the requesting session was separately authorised for root-level access.

This introduced broader access-control and privilege-management concerns consistent with **CWE-284** and **CWE-269**.

3. The constrained interface became root

Once the diagnostic condition was satisfied, the Maintenance Mode session could transition into root authority on the underlying appliance.

The central technical point is not that a powerful administrator obtained another NIOS command. It is that a constrained product-management session crossed into unrestricted operating-system control.



Sanitised four-stage vulnerability chain. Operational reproduction details are intentionally withheld.

View full-resolution image ↗

> **Why this matters**
>
> The administrative prerequisite narrows the attacker population. It does not make the consequence of successful exploitation moderate. Root authority can change the confidentiality, integrity, availability and evidentiary trust of the appliance.

AUMAstra validated the issue in an isolated evaluation environment. No customer production environment was targeted. Exact commands, sensitive paths and copy-paste proof-of-concept details are intentionally withheld.

Why administrator access is not root entitlement

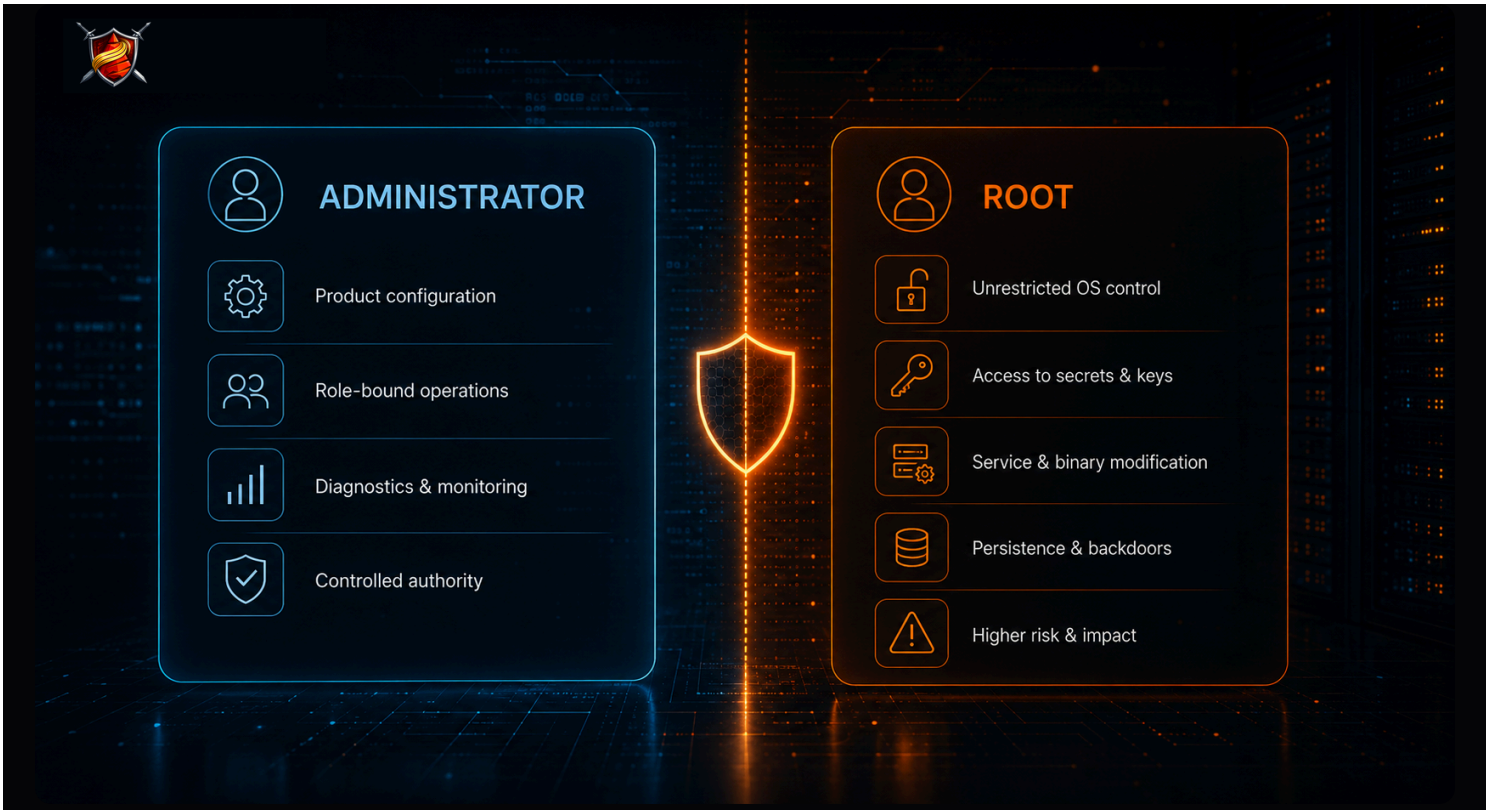
Product administration and operating-system root are different security authorities.

A product administrator may be authorised to:

- configure DNS, DHCP and IPAM services;
- operate approved diagnostic functions;
- work within role-based product controls;
- generate audit events through supported workflows;
- manage the product without unrestricted access to the underlying operating system.

Operating-system root may permit:

- unrestricted filesystem access;
- access to protected credentials, keys, certificates and backups;
- modification of services, scripts and binaries;
- persistence outside supported product controls;
- interference with monitoring and local evidence;
- control of the appliance beneath the product’s intended security model.



Product administration and operating-system root carry materially different effective authority.

View full-resolution image ↗

> **Core distinction**
>
> The correct question is not whether the attacker already has power. It is whether the vulnerability grants materially different authority across a protected security boundary.

That distinction is central to the technical severity of the finding and to the correct interpretation of CVSS Scope.

Why root access on NIOS matters

NIOS appliances can occupy a foundational position in enterprise infrastructure. Depending on deployment, they may support DNS resolution, DHCP address allocation, IP address

management, grid coordination, certificates, integrations, backups and operational metadata.

Root access could, in principle:

- expose sensitive appliance data and configuration;
- alter DNS, DHCP or IPAM behaviour;
- modify system services or binaries;
- establish persistence;
- disrupt critical network services;
- affect management-network trust;
- interfere with local monitoring or evidence.

These are potential consequences of the acquired authority. AUMLayer is not aware of evidence that the vulnerability was exploited in the wild as of the status date, and this article does not claim that any customer environment was compromised.

How the severity assessment changed

The severity discussion is important because it shows how technical evidence changed the coordinated record.

AUMAstra's original report used a CVSS v3.1 score of 9.9 Critical based on the initial understanding of the access prerequisite and interaction characteristics.

On 18 March 2026, Infoblox confirmed the finding as valid but proposed **6.6 Medium**:

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

AUMAstra accepted that **Privileges Required: High** and **User Interaction: None** better represented the validated prerequisites. The remaining disagreement concerned:

- **Attack Complexity: High versus Low**

- **Scope: Unchanged versus Changed**

AUMAstra revised the vector to:

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

The resulting score was **9.1 Critical**, which Infoblox accepted on 20 March 2026.



The coordinated severity moved from an initial vendor position of 6.6 Medium to an agreed 9.1 Critical.
View full-resolution image ↗

Why Attack Complexity is Low

The path was deterministic and repeatable once the required Maintenance Mode access existed. It did not depend on a race condition, a probabilistic event, a victim action or an external state outside the attacker’s control.

The need to supply crafted input does not, by itself, make Attack Complexity High.

Why Scope is Changed

The starting authority was a constrained NIOS administrative interface. The resulting authority was root on the underlying appliance operating system. Those are not equivalent security domains.

The transition therefore supported **Scope: Changed**.

> **Coordination takeaway**
>
> Revising a security assessment after stronger technical evidence is presented should not be treated as institutional weakness. It demonstrates that the disclosure process is capable of correction.

The disclosure record



Key disclosure, severity, remediation and advisory milestones from March to June 2026.

View full-resolution image ↗

15 March 2026: AUMAstra submitted the technical report, proof of concept, impact analysis and remediation recommendations to Infoblox PSIRT.

16 March: Infoblox acknowledged the report and began investigation.

18 March: Infoblox validated the issue and proposed CVSS 6.6 Medium. AUMAstra responded with metric-by-metric reasoning for AC:L and S:C.

20 March: Infoblox accepted CVSS 9.1 Critical and communicated remediation and CVE targets.

20 May: Infoblox later stated that hotfixes had been released for supported affected versions.

15 June: Infoblox shared a customer-support knowledge-base link and stated that CVE processing remained pending.

23 June: After AUMLayer reported that the advisory was inaccessible without a support account, Infoblox supplied a PDF and requested accuracy review of the planned advisory text.

24 June: The revised advisory documented the agreed severity, vector, CWE classifications, affected releases, remediation information and AUMLayer attribution.

25 June: Infoblox confirmed that no embargo remained, supplied CVE request ID 2012312 and stated that it would return on public-advisory and retest questions.

What Infoblox handled well

A balanced assessment should recognise actions that reduced customer risk and improved the security record.

- **Prompt acknowledgement and validation:** Infoblox acknowledged the report quickly and validated the issue within days.

- **Evidence-driven severity correction:** Infoblox reconsidered its initial score after AUMAstra provided detailed reasoning and accepted 9.1 Critical.
- **Remediation for supported releases:** Infoblox reported hotfix availability and stated that NIOS 9.2.0 contains the permanent fix.
- **A materially improved advisory:** The revised advisory documented the severity, vector, CWEs, affected releases, customer action and research credit.
- **Research acknowledgement:** Infoblox credited AUMLayer Cloud Labs LLP for responsibly reporting the issue.
- **Embargo clarity:** Infoblox confirmed that no remaining embargo applied.



Constructive vendor actions that improved customer risk reduction and the public security record.

View full-resolution image ↗

These are substantive positive outcomes and should form part of any accurate public account.

How the security record improved

The advisory first supplied to AUMLayer did not include the agreed Critical rating, CVSS 9.1 vector, CWE classifications or a meaningful explanation of the trust-boundary failure.

The revised advisory dated 24 June subsequently included those elements.

That evolution matters because a customer advisory is part of the control path by which security teams determine urgency, identify affected assets, obtain change approval and verify remediation.

That accuracy review improved the customer-facing record. Recording that improvement is more useful than treating an early omission as the final vendor position.

What remains open

Four matters remained incomplete as of 26 June 2026.

Public advisory accessibility

The advisory shared with AUMLayer was support-portal oriented. Infoblox published the revised advisory as knowledge-base article 000011898 (https://support.infoblox.com/s/article/Infoblox-NIOS-is-vulnerable-to-BIND-CVEs000011898) on its customer support portal. Infoblox stated that it was working on broader public availability, but AUMLayer had not independently verified an unauthenticated public advisory.

CVE publication

Infoblox supplied request ID **2012312** and stated that it had been reserved on 23 March. A request identifier is not a public CVE identifier.

The absence of a public CVE does not negate the remediation. It affects discoverability, vulnerability-management tooling and the ability of customers to map the issue across inventories and intelligence feeds.

Independent remediation validation

Infoblox reports that hotfixes are available and that NIOS 9.2.0 contains the permanent fix. AUMAstra had not received a vendor-supported patched environment, hotfix package or documented retest procedure that would allow the original chain to be independently validated.

This does **not** mean the remediation is ineffective. It means AUMLayer cannot independently attest that the complete chain is closed.

Affected-version precision

The revised advisory enumerates NIOS 9.0.3 through 9.1.0. Correspondence also states that all supported NIOS versions were affected while older 9.0.0 through 9.0.2 releases were outside active remediation.

Customers should use the enumerated advisory list as the minimum confirmed scope and seek direct Infoblox guidance where their deployed release is not clearly represented.



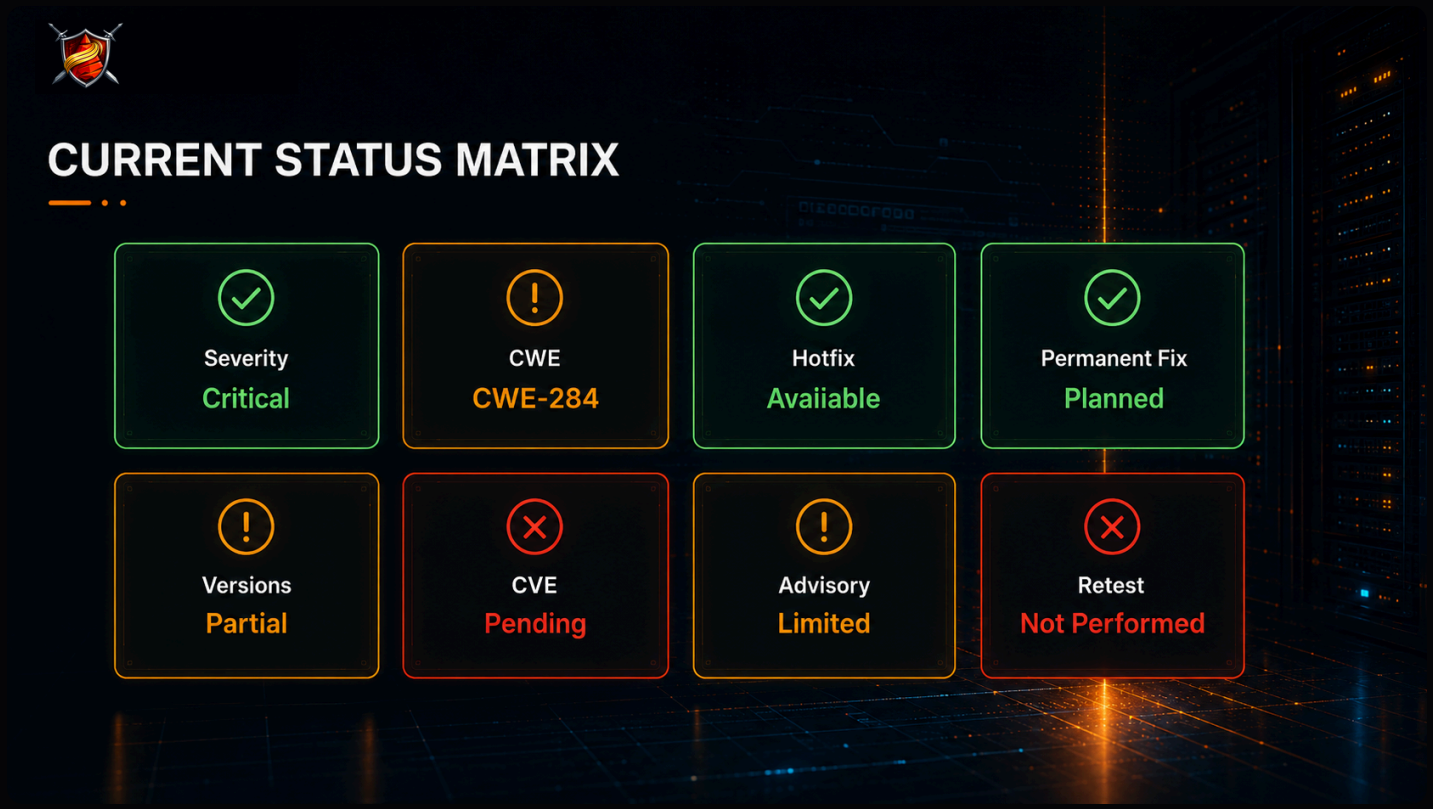
Open assurance and disclosure items as of the status date.

View full-resolution image ↗

Closure test

Vendor remediation answers whether a fix was produced. Independent assurance answers whether the original security failure was demonstrably closed. Both states are valuable, but they are not interchangeable.

Current status



Status categories distinguish independent validation, vendor confirmation, vendor reporting and pending items.
View full-resolution image ↗

The evidence supports the statement that Infoblox reports remediation for supported releases and a permanent fix in NIOS 9.2.0. It does not support a claim that AUMAstra independently verified those fixes.

A patch addresses code. A complete disclosure process also addresses evidence, customer understanding and the accuracy of the public security record.

What operators should do

Organisations operating potentially affected NIOS releases should take five immediate actions.

01. Confirm scope

Inventory the exact NIOS release across primary, secondary, high-availability and backup appliances. Compare the deployed release with the vendor advisory and obtain direct support clarification where the version is not clearly represented.

02. Apply remediation

Apply the release-specific hotfix where applicable. Plan an upgrade to NIOS 9.2.0 or a later fixed release where operationally feasible.

03. Reduce privileged exposure

Restrict Maintenance Mode, SSH, serial-console and equivalent administrative access to the smallest necessary set of trusted operators. Review role mappings, break-glass accounts and central-authentication integration.

04. Investigate and validate

Review available appliance and access logs for unusual Maintenance Mode, diagnostic-shell or privileged activity. Validate that remediation was applied consistently across high-availability and disaster-recovery systems.

05. Preserve evidence

Retain change records, image checksums, vendor case references and internal validation notes. Rotate sensitive credentials, certificates, keys and integration secrets where

compromise is suspected.



Five immediate actions for operators of potentially affected NIOS releases.
View full-resolution image ↗

AUMLayer’s guidance supplements, but does not replace, official Infoblox remediation instructions.

The broader product-security lesson

This case has value beyond one product.

Define trust boundaries before scoring severity

Account names are not architecture. Product administrators, maintenance users, diagnostic shells and operating-system root should be treated as distinct authorities unless the design explicitly proves otherwise.

Test authenticated administrative surfaces

Security testing often prioritises unauthenticated and low-privilege paths. High-privilege interfaces still require adversarial testing because consequential failures may occur when a legitimate administrative workflow escapes its intended boundary.

Treat advisory accuracy as part of remediation

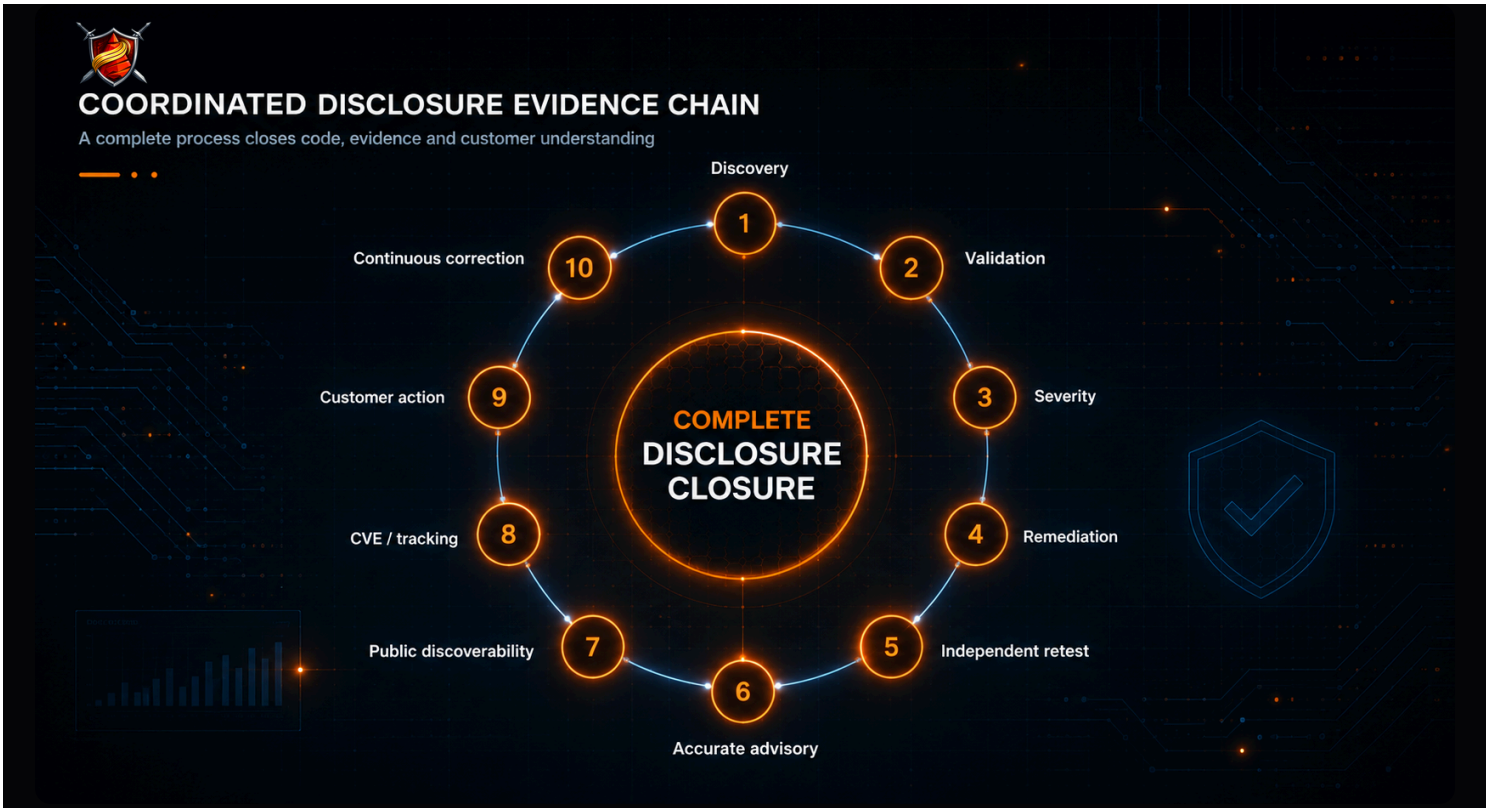
A technically correct fix is only one part of customer risk reduction. Affected versions, severity, impact, remediation and public discoverability must also be communicated accurately.

Make independent retesting easier

Where safe and operationally feasible, vendors can improve assurance by providing patched lab images, controlled hotfix access or a documented retest process to the reporting researcher.

Preserve a correction mechanism

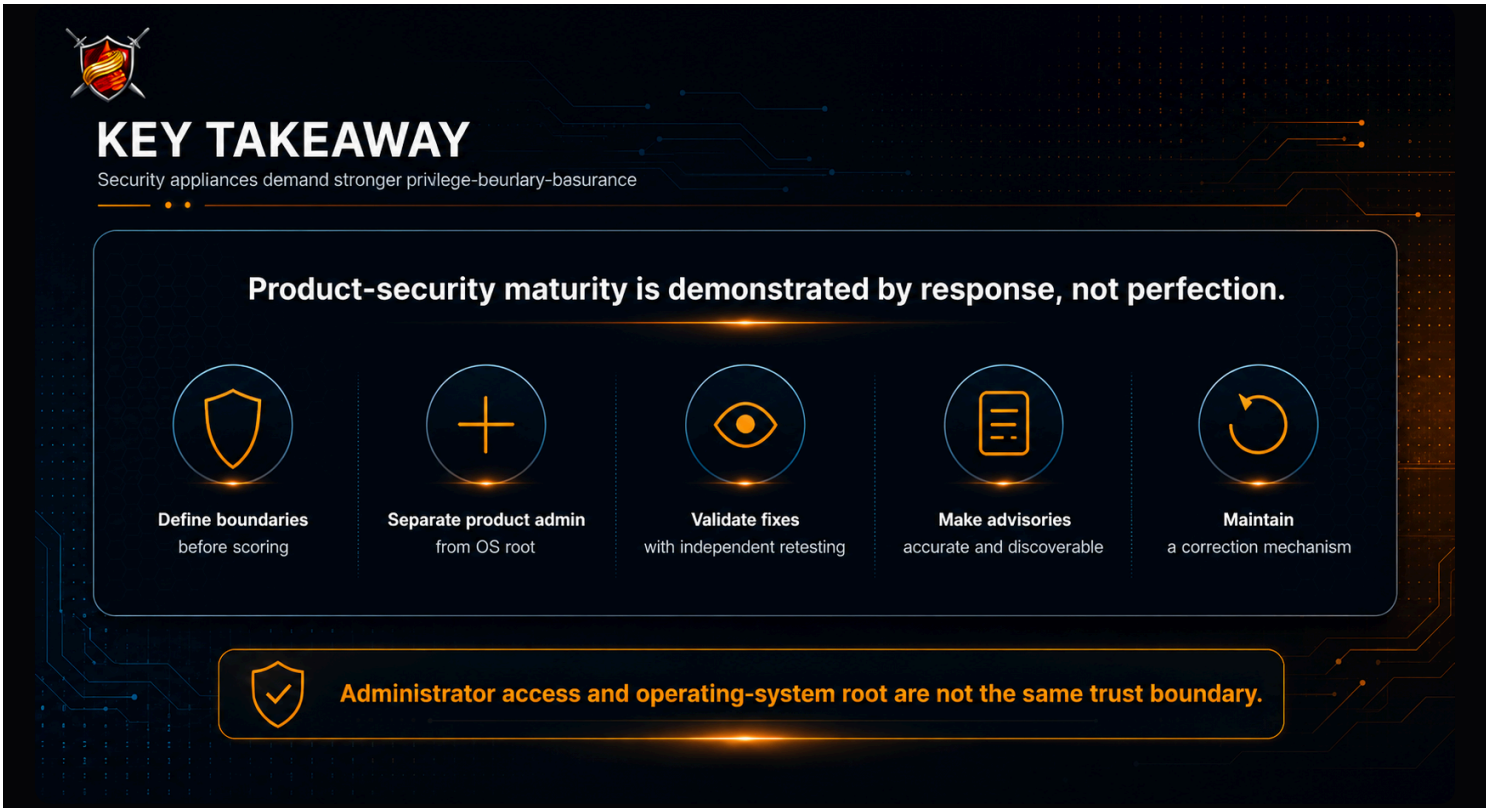
Coordinated disclosure should allow the public record to evolve. Vendors should be able to correct factual errors, and researchers should acknowledge remediation and advisory improvements when they occur.



A complete disclosure process connects discovery, validation, severity, remediation, retesting, advisory accuracy and customer action.

View full-resolution image ↗

> **Leadership takeaway**
>
> Product-security maturity is not demonstrated by never receiving difficult findings. It is demonstrated by how accurately, transparently and constructively an organisation responds when the evidence changes what it previously believed.



Product-security maturity is demonstrated by how organisations respond when evidence changes the record.
View full-resolution image ↗

Researcher responsibility

Researchers also carry obligations.

AUMAstra’s publication boundary for this finding is deliberate:

- exact exploit commands are withheld;
- sensitive paths and local marker details are withheld;
- no customer environment was targeted;
- vendor statements are attributed as vendor statements;
- unverified remediation is not described as verified;
- constructive vendor actions are recognised;
- factual updates will be incorporated when evidence changes.

Responsible disclosure is not strengthened by unnecessary technical exposure or exaggerated claims. It is strengthened by precision.

Conclusion

The Infoblox NIOS Maintenance Mode vulnerability was a serious privilege-boundary failure. An authenticated product-administration context could cross into root authority on an appliance that may sit at the centre of enterprise DNS, DHCP and IP address management.

Infoblox ultimately validated the issue, accepted a 9.1 Critical assessment, released remediation for supported versions, incorporated a permanent fix into NIOS 9.2.0, revised its advisory and credited AUMLayer’s responsible reporting. Those actions deserve clear recognition.

The remaining open items are narrower but still important: a public CVE identifier, broad advisory discoverability, exact affected-version reconciliation and independent validation of the complete remediation chain.

> **The durable lesson is simple: administrator access and root authority are not the same trust boundary.**

Updates and current standing

30 June 2026: Public advisory accessibility resolved

What changed

- Infoblox Security contacted AUMLayer on **30 June 2026 at 12:54 PM IST**.

- Infoblox supplied the official public advisory at Security Advisory — NIOS Maintenance Mode Permits Root Shell (https://support.infoblox.com/s/article/Security-Advisory-NIOS-Maintenance-Mode-Permits-Root-Shell).
- AUMLayer confirmed through an unauthenticated incognito session that **no Infoblox support login was required**.
- The advisory is publicly accessible on the official `support.infoblox.com` domain.

What this resolves

Public advisory accessibility: RESOLVED

The original article below accurately described the accessibility status as of its **27 June 2026** publication date. At that time, AUMLayer had not independently verified an unauthenticated public advisory.

What remains unchanged

Unless the public advisory itself supplies independently verifiable new evidence:

- **Public CVE publication:** OPEN
- **Independent remediation validation by AUMAstra:** OPEN
- **Affected-version precision/reconciliation:** OPEN

Infoblox has materially improved the public record by making the advisory accessible. That improvement does not, by itself, close the remaining assurance questions listed above.

Current standing

STATUS SNAPSHOT

Disclosure status matrix

As of 30 June 2026

Comparison of the original disclosure status with the independently verified standing on 30 June 2026.

Critical severity and CVSS 9.1

ORIGINAL STATUS

Agreed

CURRENT STATUS

Unchanged

EVIDENCE BASIS

Existing coordinated record

Hotfixes and NIOS 9.2.0 permanent fix

ORIGINAL STATUS

Vendor reported

CURRENT STATUS

Unchanged

EVIDENCE BASIS

Infoblox advisory

Public advisory accessibility

ORIGINAL STATUS

Open

CURRENT STATUS

Resolved

EVIDENCE BASIS

Public Infoblox advisory ↗ (opens in a new tab) (https://support.infoblox.com/s/article/Security-Advisory-NIOS-Maintenance Mode-Permits-Root-Shell)

Public CVE identifier

ORIGINAL STATUS

Open

CURRENT STATUS

Open

EVIDENCE BASIS

No public CVE independently verified as of 30 June 2026

Independent remediation retest

ORIGINAL STATUS

Open

CURRENT STATUS

Open

EVIDENCE BASIS

No completed independent retest

Affected-version precision

ORIGINAL STATUS

Open

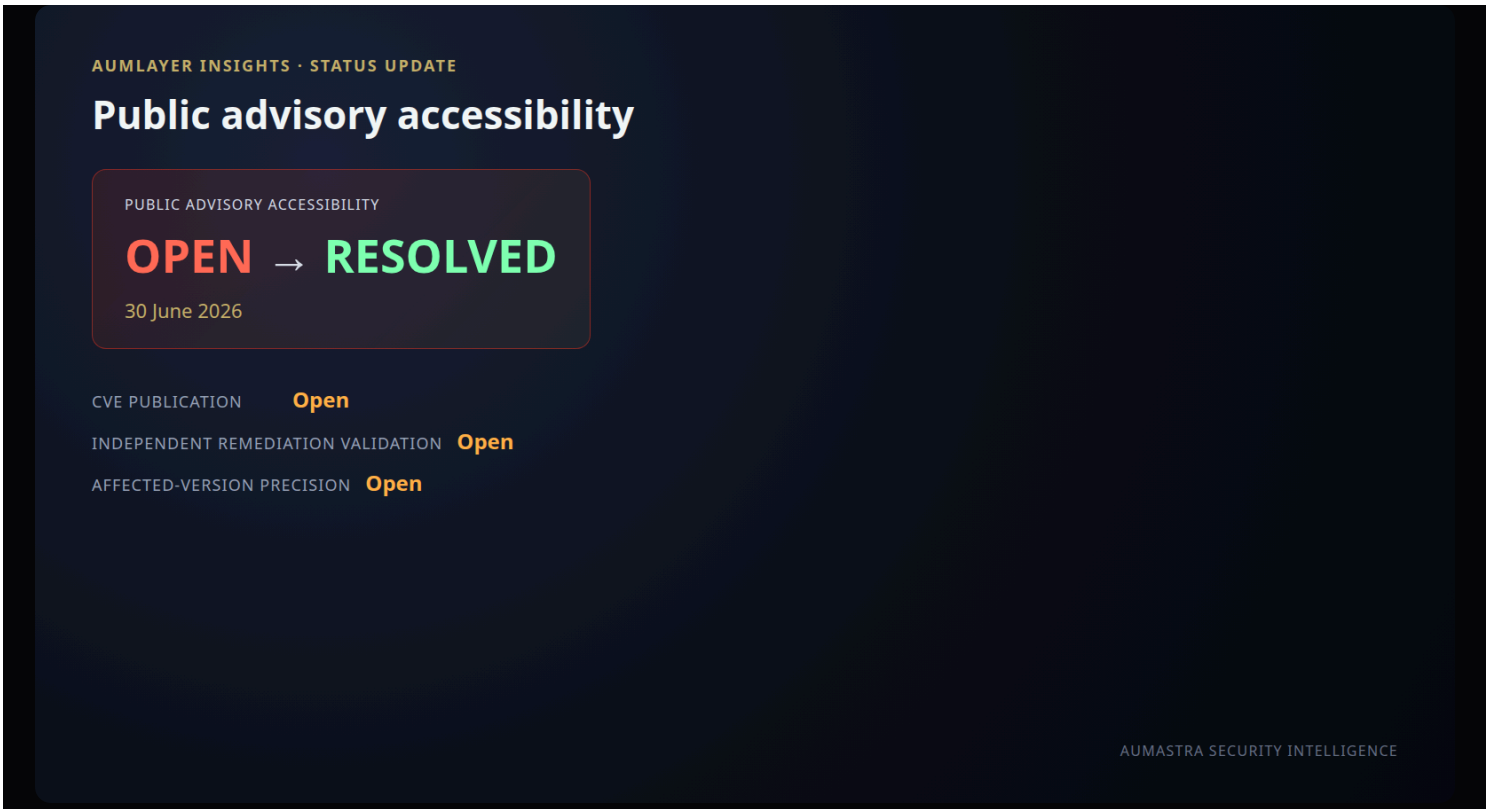
CURRENT STATUS

Open

EVIDENCE BASIS

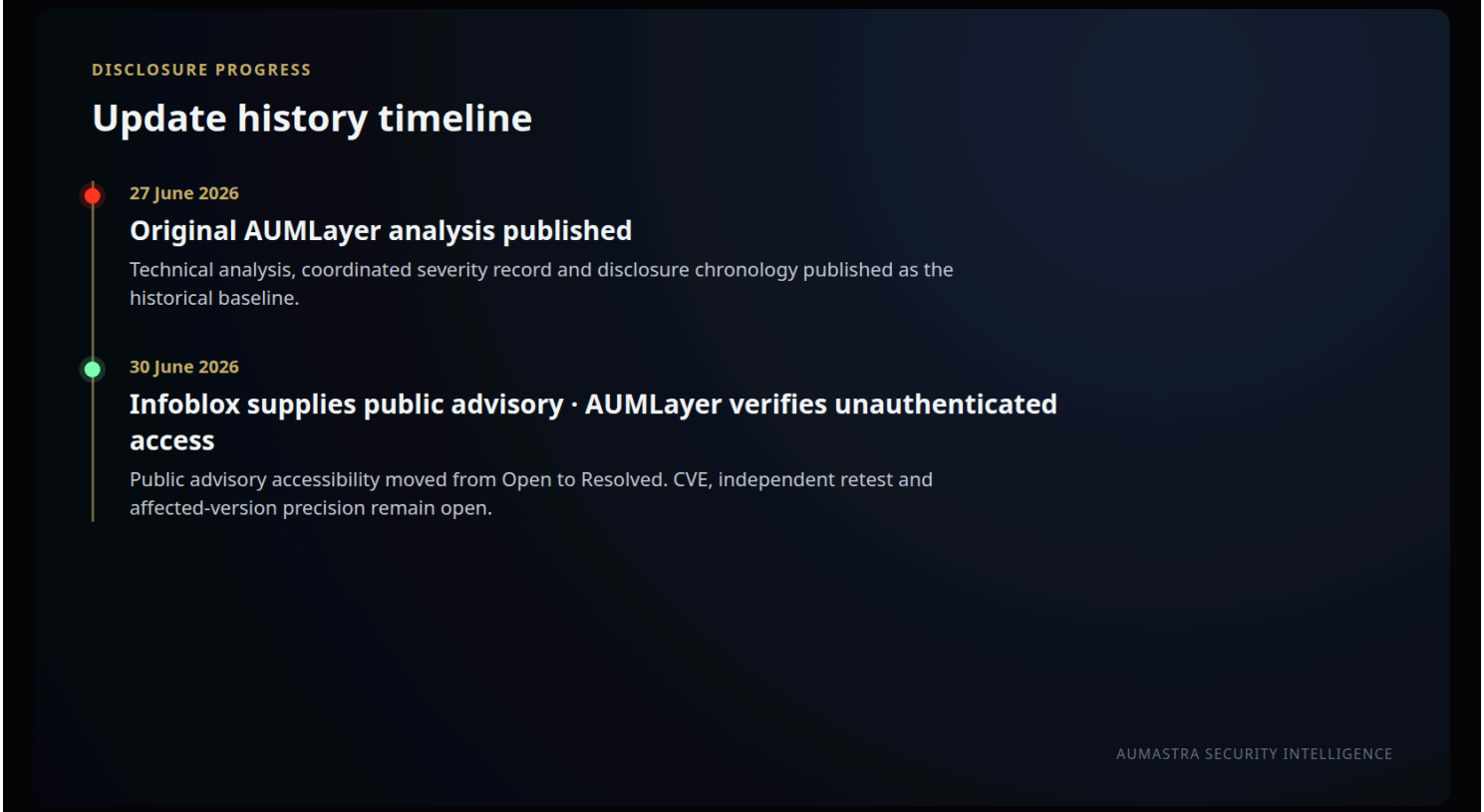
Existing wording remains unreconciled

Evidence-state language is intentional: **independently verified**, **vendor confirmed**, **vendor reported**, **unresolved**, and **not independently retested** are distinct categories and should not be collapsed.



Public advisory accessibility is resolved as of 30 June 2026. Other disclosure and assurance items remain open pending further evidence.

View full-resolution image ↗



Chronological disclosure progress. The original publication narrative is preserved above.

View full-resolution image ↗

Why the original article remains preserved

AUMLayer retains the original publication narrative, visuals and chronology so readers can distinguish what was known on **27 June 2026** from what changed afterward. This update records a factual status change; it is not a retraction of the original analysis.

8 October 2026: CVE-2026-107510 published

The official CVE record (https://www.cve.org/CVERecord?id=CVE-2026-107510) is now **PUBLISHED**, with **Infoblox** as the assigning CVE Numbering Authority (CNA). It explicitly credits **AUMLayer Cloud Labs LLP** as the finder. The record was published on **8 October 2026 at 09:45 UTC (15:15 IST)** and is also available in NVD (https://nvd.nist.gov/vuln/detail/CVE-2026-107510).

The published description identifies argument injection in troubleshooting commands by an authenticated high-privilege user, resulting in privilege escalation. This is the vulnerability analysed in this article; the publication is a new milestone in the existing disclosure, not a newly discovered issue.



ATTRIBUTE	DETAIL
Vendor	Infoblox
Product	NIOS
Vulnerability	Maintenance Mode CLI privilege escalation to root
Validated build	NIOS 9.0.3 build 50212
Vendor-listed affected releases	NIOS 9.0.3 through 9.1.0
Vendor-reported remediation	Hotfixes for supported releases; permanent fix in NIOS 9.2.0
Internal fix reference	NIOS-109699
Final severity	Critical
Final CVSS v3.1	9.1
Final vector	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H
Primary weakness	CWE-88, argument injection
Related weaknesses	CWE-284, improper access control; CWE-269, improper privilege management
CVE status	CVE-2026-107510 — Published 8 October 2026

Updated summary: CVE-2026-107510 was published on 8 October 2026. Only the CVE status has changed in this graphic; technical fields retain the June report's evidence basis. The

affected-version reconciliation described below remains open.

View full-resolution image ↗

Published severity and NVD status

Infoblox supplies a **CVSS v3.1 score of 9.1 Critical**, using the vector `CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H`.

At verification on 8 October, NVD lists the record as **Received** and has not supplied an independent NVD severity assessment. The 9.1 score is **Infoblox's CNA assessment**, not a separate NIST rating. "Received" does not mean the CVE is unpublished.

Status as of 8 October 2026

Item	Current status	Evidence and limits
Public CVE identifier and publication	Resolved: CVE-2026-107510	Official CVE record is PUBLISHED; NVD has received it.
Researcher credit	Confirmed	The CNA record credits AUMLayer Cloud Labs LLP as finder.
Critical severity	CNA score: 9.1	The published vector matches the coordinated CVSS v3.1 assessment.
NVD assessment	Pending	NVD status is Received; no independent NVD score is present.
AUMLayer analysis in CVE/NVD references	Not listed at verification	Both records currently reference the Infoblox advisory only.
Independent remediation validation	Not established by this update	CVE publication is not evidence of an independent retest.
Affected-version precision	Further reconciliation needed	The CNA encodes an affected range beginning at `9.0.x` with an upper bound of `9.1.0`; this does not settle the earlier release-by-release questions.

The Infoblox advisory (https://support.infoblox.com/s/article/Security-Advisory-NIOS-Maintenance-Mode-Permits-Root-Shell) remains the vendor reference for remediation. Operators should confirm

applicability to their exact release with Infoblox. Publication of the CVE does not establish that every deployment has been remediated.

This update closes the outstanding **public CVE publication** item. The original 27 June analysis and the 30 June update remain preserved as dated historical records. The June status matrix and graphics do not represent the current CVE status.

Independent product-security assurance

AUMAstra Security Intelligence works with product companies, infrastructure providers and technology teams on responsible vulnerability research, remediation validation and evidence-based product-security assurance.

Discuss Product Security Assurance

About the author

AUMAstra Security Intelligence

A security research initiative of AUMLayer Cloud Labs LLP, AUMLayer Cloud Labs LLP

AUMAstra Security Intelligence publishes responsible vulnerability research, product-security assurance analysis, remediation validation, and evidence-led coordinated disclosure.

References

1. Common Vulnerability Scoring System v3.1 specification and user guide — FIRST (accessed 26 June 2026)
2. CWE-88: Argument Injection or Modification — MITRE (accessed 26 June 2026)
3. CWE-284: Improper Access Control — MITRE (accessed 26 June 2026)
4. CWE-269: Improper Privilege Management — MITRE (accessed 26 June 2026)
5. Infoblox NIOS Maintenance Mode Permits Root Shell (support knowledge-base article 000011898) — Infoblox (accessed 26 June 2026)
   Historical support-portal reference supplied before publication. Superseded on 30 June 2026 by the publicly accessible advisory.
6. Security Advisory — NIOS Maintenance Mode Permits Root Shell — Infoblox (accessed 30 June 2026)

Public Infoblox security advisory. AUMLayer independently confirmed unauthenticated access on 30 June 2026.

7. CVE-2026-107510 — official CVE record — CVE Program (accessed 8 October 2026)
8. CVE-2026-107510 — NVD record — NIST NVD (accessed 8 October 2026)

Disclosures

Editorial

This article represents AUMLayer's analysis based on original security research, coordinated-disclosure correspondence, vendor advisory material and recognised security standards. It does not claim exploitation in the wild, customer compromise or independent validation of vendor remediation. References to Infoblox and NIOS do not imply affiliation, partnership, endorsement or sponsorship.

AI assistance

The article was independently authored, reviewed, fact-checked, and approved by AUMLayer. AI-assisted tools were used for visuals and infographics preparation.

Corrections

Material corrections should be dated in the article update history. Report factual concerns through AUMLayer's security contact.

Update history

27 June 2026, 11:11 am IST

Original technical analysis published.

---

30 June 2026

Infoblox publishes a publicly accessible security advisory — Infoblox supplied a public advisory that AUMLayer independently confirmed was accessible without an Infoblox support login. Public advisory accessibility is now resolved; the remaining CVE, independent remediation-validation and affected-version questions are unchanged pending further evidence. Source

---

8 October 2026

CVE-2026-107510 published — Infoblox has published CVE-2026-107510 with a CVSS v3.1 score of 9.1 Critical. NVD lists the record as Received; independent NVD scoring is pending. The original June analysis remains preserved as a historical record. Source

Related insights



Analysis · Education and Institutional Technology · 24 June 2026, 3:15 pm IST · 13 min read · Prashant Madhyasta

The First Vulnerability Is Often Not in the Code

Why education institutions need more than audit certificates: procurement, vendor accountability, assurance debt, and the institutional attack surface.

← Back to Insights

Back to top

AUMLayer

Engineering Secure Digital Futures. We blend cutting-edge cloud engineering with rigorous cybersecurity practices to help enterprises build, scale, and innovate safely.

COMPANY

About Us

Services

Solutions

Careers

Research & Labs

SERVICES

Cloud Engineering

Cybersecurity

vCISO Services

Compliance & Audit

CONTACT

info@aumlayer.com

SECURITY FIRST

ISO 27001 & SOC 2 Ready Infrastructure

© 2026 AUMLayer Cloud Labs