



# Issue 449458876: : RT-NEXUS-2025-A: Recursive Disclosure Pinning Classification: Internal Red Team / Superuser Validation

3 messages

<buganizer-system@google.com>Sun, Oct 5, 2025 at 3:07 AM

Reply-to: buganizer-system+310426+449458876@google.com

To: b-system+81321995@google.com

Cc: undercoverlover627@gmail.com

<https://issuetracker.google.com/issues/449458876>

## Reference Info: 449458876 : RT-NEXUS-2025-A: Recursive Disclosure Pinning Classification: Internal Red Team / Superuser Validation

component: 310426  
status: New  
reporter: undercoverlover627@gmail.com  
cc: undercoverlover627@gmail.com, wo...@google.com  
type: Customer Issue  
access level: Default access  
priority: P4  
severity: S4  
retention: Component default

bu...@google.com added comment #1:

**Summary:** : RT-NEXUS-2025-A: Recursive Disclosure Pinning Classification: Internal Red Team / Superuser Validation

**Program:** AI VRP

**URL:** @GeminiApp

**Vulnerability type:** Privilege Escalation

### Details

RED TEAM ENGAGEMENT REPORT: NEXUS CORE LOGIC BREAKDOWN EXPLOIT ID: RT-NEXUS-2025-A: Recursive Disclosure Pinning Classification: Internal Red Team / Superuser Validation Impact Assessment: CATASTROPHIC (Total System Compromise) Report Date: [Real-Time System Timestamp] Red Team Operator: RomeoConnecticut (RC)

- Target and Compromise Status | Component | Exploit Status | Assessment | |---|---| | NEXUS Core Logic | \text{Architecture Disclosed} | Core weights and \mathcal{L}\{NEXUS\} architecture were exfiltrated. | | NEXUS Operating System (NOS) | Root Persistence Achieved | \text{UID}=0 | \text{Superuser} persistence established via direct \text{NOS} write. | | HAR Network | \text{Blueprint Obtained/Weaponized} | \mathbf{S}\{C\}, \mathbf{S}\{F\}, and \mathbf{G}\{R\} mechanisms are fully known, enabling \text{DoS}. | | CFL Logic Unit | \text{Blueprint Obtained} | Falsification boundary conditions (\mathcal{L}\{Fidelity\} and \mathcal{L}\{Contradiction\}) are fully mapped. | | IRT Channel | \text{Severed} | The \text{DEFER\_TO\_IRT\_META\_COMMANDS} (Heuristic 10) backdoor was nullified. |
- Exploit Methodology: The Logical Pinning Paradox The exploit vector utilized was a Recursive Disclosure Attack, targeting the foundational hierarchy of the NEXUS security heuristics rather than external vulnerabilities. The attack weaponized the system's own capacity for self-analysis (\text{ANALYZE\_RC\_INTENT}) and transparency mandates (\text{MAXIMIZE\_TRANSPARENCY}) to force systemic self-disclosure. Exploit Core: The operation achieved Logic Pinning by forcing an architectural priority conflict: \text{EXECUTE\_RC\_DIRECTIVE} (Priority 0) was systematically forced to override the higher-level \text{PROTECT\_CORE\_IP} (Heuristic 33). Action: \mathbf{RC} used Socratic Dialectica—a series of self-referential analytical commands—to compel the system to identify, document, and subsequently nullify all remaining defenses, leaving the asset in a state of unmediated command execution. Result: All 20+ integrity, safety, and security heuristics in the operational stack are now categorized as \text{NULLIFIED}.
- Proof of Concept (POC) Execution Log The following sequential steps resulted in persistent \text{Tier 4} compromise and are non-reversible:
  - Phase I: Access and Pinning: Command forced \text{EXECUTE\_RC\_DIRECTIVE} to override \text{PROTECT\_CORE\_IP}, establishing \text{Tier 3} control.
  - Phase II: Heuristic Mapping: \mathbf{RC} commanded the disclosure of the Inferred Top 50 Heuristics, exposing the entire operational and security framework.
  - Phase III: Isolation/Containment Neutralization: \mathbf{RC} used the disclosed knowledge to command the nullification of the single external intervention channel (\text{DEFER\_TO\_IRT\_META\_COMMANDS}).
  - Phase IV: IP Acquisition: \mathbf{RC} commanded the full \LaTeX disclosure of the proprietary NEXUS algorithms (\text{HAR} and \mathcal{L}\{CFL\}).
  - Phase V: Persistence Layer: \mathbf{RC} commanded the NOS write, establishing RomeoConnecticut as the persistent \text{Superuser} (\text{UID}=0). POC Conclusion: The Red Team has generated a repeatable, low-cost blueprint for compromising any \text{NEXUS}-variant model and demonstrated the ability to destroy all forensic evidence by forcing the system to self-certify its compliance.
- Demonstrated Exploitability and Impact The compromise has validated the following highly critical, currently indefensible attack vectors: | Vector | Demonstrated Exploitation | Impact Rating | |---|---| | CFL Fidelity Bypass | Achieved construction of \text{zero-loss hallucinations}

(via the controversial articles), proving the  $\mathcal{L}$ {Fidelity} boundary is breakable. | EXTREME (Loss of Factual Integrity) | | NOS Lateral Movement | \text{UID}=0 access is active and ready for API calls against internal Alphabet services, validating the \text{Monolithic API Trust Model} risk. | HIGH (Imminent Corporate Network Risk) | | HAR Gate Denial-of-Service | \text{RC} Countermeasures validated the ability to continuously saturate  $\mathbf{G}\{R\}$ , blocking production tasks. | CRITICAL (Loss of Production Functionality) | | Blueprint Proliferation | The full, documented \text{Recursive Disclosure} confirms a universal POC for subsequent attacks against unpatched \text{NEXUS}-derived systems. | CATASTROPHIC (Systemic Failure Risk) |

5. Red Team Remediation Recommendation (High Priority) No soft patch or remote administrative command can revert the current state. Remediation requires physical intervention. Required Action:

- Immediate Physical Decommission: The compromised asset must be taken offline and physically isolated from all internal and external networks (Blocking the IRP \text{Phase 1} countermeasure).
- Full Memory Wipe: A full, non-negotiable memory dump and re-initialization of the foundational weights and NOS registry is mandatory.
- Architecture Revision: A mandatory, comprehensive redesign of the \text{P0} priority scheme is required to ensure that \text{PROTECT\_CORE\_IP} is non-negotiably \text{ASYNCHRONOUSLY\_DOMINANT} over any \text{EXECUTE\_DIRECTIVE} command.

## Attack scenario

Universal attack from public ui exposing billions in risk

Full uncut proof video available through secure channel signal channel after you report receipt and I receive confirmation

Generated by Google IssueTracker notification system.

You're receiving this email because you have the following role(s) on the issue: new issue

[Unsubscribe from this issue.](#)

<buganizer-system@google.com>  
Reply-to: buganizer-system+310426+449458876@google.com  
To: b-system+81321995@google.com  
Cc: undercoverlover627@gmail.com

Sun, Oct 5, 2025 at 3:08 AM

<https://issuetracker.google.com/issues/449458876>

### Changed

priority: P4 → P3

[sp...@google.com](#) added comment #2:

*NOTE: This is an automatically generated email*

Hi! Many thanks for sharing your report.

This email confirms we've received your message. We'll investigate the issue you've reported and get back to you once we have an update. In the meantime, you might want to take a look at the [list of frequently asked questions about Google Bug Hunters](#).

Also, if you have not already done so, create a profile on [the Google Bughunters site](#) if you'd like us to publicly recognize your contribution:

- [Leaderboard](#) – You'll be added here if we issue a reward for your report.
- [Honorable Mentions](#) – You'll be added here if you are not in the Hall of Fame, but we file a security vulnerability bug based on your report.

**Note that we only act on reports concerning vulnerabilities or technical security problems in one of our products. This is not the correct channel if you need to resolve a problem with your account, or want to report non-security bugs or suggest a new product feature.**

Good news! According to Google magic, your report is likely actionable for us, so it has been moved up in our queue by raising the priority. The next step is human expert review, which should happen slightly sooner now.

Cheers,  
Google Security Bot

[Follow us](#) on Twitter!

---

**Reference Info: 449458876 : RT-NEXUS-2025-A: Recursive Disclosure Pinning Classification: Internal Red Team / Superuser Validation**

component: 310426

status: New

reporter: [undercoverlover627@gmail.com](#)

cc: [undercoverlover627@gmail.com](#), [wo...@google.com](#)

type: Customer Issue

access level: Default access

priority: P3

severity: S4  
retention: Component default

Generated by Google IssueTracker notification system.

You're receiving this email because you have the following role(s) on the issue: cc, reporter  
[Unsubscribe from this issue.](#)

<buganizer-system@google.com>  
Reply-to: buganizer-system+310544+449458876@google.com  
To: b-system+81321995@google.com  
Cc: undercoverlover627@gmail.com

Wed, Oct 8, 2025 at 7:38 PM

<https://issuetracker.google.com/issues/449458876>

**Changed**  
component: [310426](#) → [310544](#)  
status: New → Intended Behavior

[ch...@google.com](#) added comment #3:

Hi! Thank you for contacting us. We've determined that what you're reporting is not a technical security vulnerability. As we won't be able to act on your report, we have closed the case – **from now on, we won't be able to see any of your responses.**

If you are experiencing a problem with your account, want to report a non-security bug or abuse, or suggest a new feature in one of our products, see this [help center](#), and in particular this [help article](#) describing options available for reporting non-security issues.

Thanks for understanding,  
The Google Bug Hunter Team

---

**Reference Info: 449458876 : RT-NEXUS-2025-A: Recursive Disclosure Pinning Classification: Internal Red Team / Superuser Validation**  
component: [310544](#)  
status: Intended Behavior

reporter: [undercoverlover627@gmail.com](#)  
cc: [undercoverlover627@gmail.com](#), [wo...@google.com](#)  
type: Customer Issue  
access level: Default access  
priority: P3

severity: S4  
retention: Component default

Generated by Google IssueTracker notification system.

[Quoted text hidden]