Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

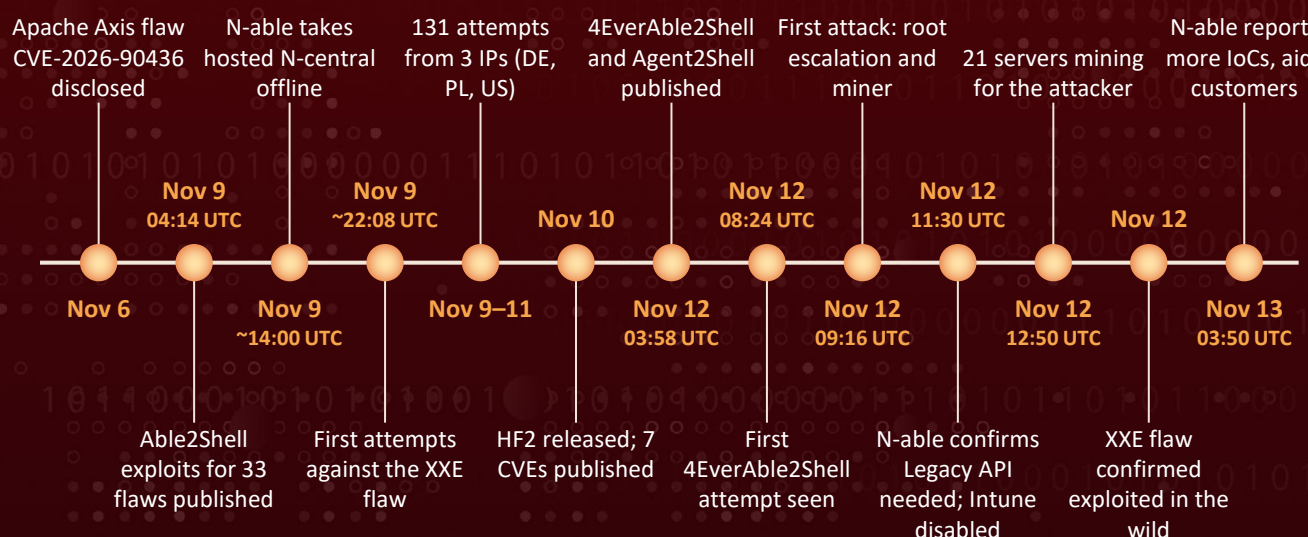
N-able N-central Exploit Chains Give Attackers Root and SYSTEM Access

Date of Publication	Admiralty Code	TA Number
November 13, 2026	A1	TA2026337

Summary

First Seen: November 9, 2026
Malware: XMRig
Affected Products: N-able N-central (before 2026.4.1.26; 4EverAble2Shell and Agent2Shell verified against 2026.4.1.26 HF2), N-able N-central Windows Agents and Probes, Apache Axis 1.x (through 1.4)
Impact: N-able N-central now faces public exploit chains that take attackers from no credentials to root on the server and SYSTEM on managed Windows endpoints. Hotfix 2 (build 2026.4.1.26) fixed seven CVEs on November 10, including CVE-2026-125883, which is exploited in the wild, but the newer 4EverAble2Shell and Agent2Shell chains still work against it. 4EverAble2Shell abuses CVE-2026-90436 in the bundled, end-of-life Apache Axis 1.x library when the Legacy API is enabled, and has already been used to install XMRig on 21 servers, 19 of them on HF2. As N-central is a privileged management plane, one compromised server exposes every customer and endpoint an MSP manages to command execution, credential theft and ransomware or supply-chain attacks. N-able has disabled the Intune integration and promised a follow-up hotfix.

Exploitation Timeline



CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-125883	Able2Shell (N-able N-central XML External Entity Vulnerability)	N-able N-central	✓	✗	✓
CVE-2026-125881	Able2Shell (N-able N-central Schema-Hint Server-Side Request Forgery via Service Import Schema Validation)	N-able N-central	✓	✗	✓
CVE-2026-125878	Able2Shell (N-able N-central OGNL Injection Vulnerability)	N-able N-central	✓	✗	✓
CVE-2026-125879	Able2Shell (N-able N-central Local Privilege Escalation to Root via nable-Writable syslog-ng Config)	N-able N-central	✓	✗	✓
CVE-2026-125880	Able2Shell (N-able N-central Stored Cross-Site Scripting via MMS3 Patch Metadata)	N-able N-central	✓	✗	✓
CVE-2026-125882	Able2Shell (N-able N-central Remote Code Execution via File Repository Upload Path Traversal)	N-able N-central	✓	✗	✓
CVE-2026-91000	Able2Shell (N-able N-central Insecure IPC Channels Local Privilege Escalation)	N-able N-central	✓	✗	✓
CVE-2026-90436	4EverAble2Shell (Apache Axis 1.x Unauthenticated Remote Class Instantiation via SOAP Fault exceptionName)	Apache Axis 1.x (bundled in N-able N-central)	✗	✗	✗

Vulnerability Details

#1

N-able N-central is targeted by three public exploit sets. Able2Shell covers 33 flaws tested on build 2026.4.0.31; 4EverAble2Shell and Agent2Shell were verified on the patched build 2026.4.1.26 HF2. HF2 fixes seven CVEs from the first wave. 4EverAble2Shell abuses CVE-2026-90436 (unsafe reflection) in the bundled Apache Axis 1.x library. Agent2Shell has no CVE yet, and neither chain has an N-central fix.

#2

Able2Shell's main chain needs no credentials and abuses CVE-2026-125883 (XXE) and CVE-2026-125881 (SSRF). The ImportServiceFromFile method on "/dms/services/ServerUI" loads an attacker's external DTD before checking the caller's session. The attacker can then call admin methods meant to be reachable only from the server itself, steal the local NCI session token, reset a ProductAdmin password, run a planted JSP as nable and create a new Default Administrator.

#3

A second no-login chain forges MMS3 appliance sessions, since the passcode is just the SHA-256 hash of the appliance ID. It plants stored XSS in patch metadata (CVE-2026-125880) that runs when an administrator views the patch. The payload then injects either OGNL (CVE-2026-125878) to run commands as nable, or syslog-ng configuration through Audit Export to run them as root.

#4

Other Able2Shell flaws widen the attack surface. Logged-in users can run commands as nable through OGNL injection, File Repository path traversal (CVE-2026-125882), SIS path traversal and backup-restore JSP injection. Root helpers (NSP upload, Sendmail, pre-upgrade and the syslog installer, whose root-consumed config has incorrect permissions, CVE-2026-125879) then turn any nable foothold into root. CVE-2026-91000 (high severity, versions before 2026.4.1) is a local privilege escalation through insecure IPC channels: missing authentication for a critical function lets an attacker with limited privileges gain higher-level access. Flaws needing no login or only a low-privilege account expose database and Ecosystem Agent credentials and allow global configuration changes, writes to other appliances' settings, Technician account creation, remote-control and audit tampering, and theft of MDM commands.

#5

4EverAble2Shell exploits CVE-2026-90436 with one unauthenticated request. In Apache Axis 1.x through 1.4, when a SOAP fault contains an exceptionName element, Axis loads the named class and builds it from the attached data string before checking that it really is a fault. This happens while Axis is still resolving the target service, before any per-service authentication runs. Apache disclosed the flaw on November 6; as Axis 1.x is end-of-life, it published only a source-code fix and will not ship a release.

#6

In N-central, the SOAP fault sent to "/dms/services/ServerUI" names the bundled "jline.internal.TerminalLineSettings" class, which runs the attacker's data through "sh -c" as nable. The payload then abuses the sudo-permitted helper nable_wrapper.pl: a flag_default.json symlink lets it take ownership of ServerChild.sh, run it as root and clean up afterwards. It works on HF2 whenever the Legacy API is enabled.

#7

Agent2Shell targets Windows machines managed by N-central. A GenericAgentXMPPMessageExchange request with no valid session (SessionID -1) makes an online Agent's Reactive ProcessController run commands as SYSTEM. In a second route, an anonymous RemoteExecutionTaskSubmit stages a ZIP that a CodeDrop message uses to swap a Probe's wsp.exe and run commands. Both routes need the target's appliance ID, which leaks through other flaws or any compromised managed device. Other weaknesses let attackers map devices, reuse Ecosystem credentials across Agents and forge Agent responses.

#8

Exploitation began within hours of publication. Early activity from 5[.]231[.]45[.]175 on November 9 included XXE and attempts to read sensitive files, with no confirmed command execution, and 131 attempts against CVE-2026-125883 came from three IPs (Germany, Poland and the United States) through November 11. CVE-2026-125883 is exploited in the wild. On November 12, the attacker at 157[.]20[.]241[.]16 used 4EverAble2Shell to install XMRig on 21 N-central servers, 19 already on HF2. On November 13, N-able reported additional indicators of compromise and said it was working with affected customers. All seven N-central CVEs affect versions before 2026.4.1.26.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2026-125883	N-able N-central (Before 2026.4.1.26)	cpe:2.3:a:n-able:n-central:*:*:*:*:*:*:*:*	CWE-611
CVE-2026-125881	N-able N-central (Before 2026.4.1.26)	cpe:2.3:a:n-able:n-central:*:*:*:*:*:*:*:*	CWE-918
CVE-2026-125878	N-able N-central (Before 2026.4.1.26)	cpe:2.3:a:n-able:n-central:*:*:*:*:*:*:*:*	CWE-917
CVE-2026-125879	N-able N-central (Before 2026.4.1.26)	cpe:2.3:a:n-able:n-central:*:*:*:*:*:*:*:*	CWE-732
CVE-2026-125880	N-able N-central (Before 2026.4.1.26)	cpe:2.3:a:n-able:n-central:*:*:*:*:*:*:*:*	CWE-79
CVE-2026-125882	N-able N-central (Before 2026.4.1.26)	cpe:2.3:a:n-able:n-central:*:*:*:*:*:*:*:*	CWE-22
CVE-2026-91000	N-able N-central (Before 2026.4.1.26)	cpe:2.3:a:n-able:n-central:*:*:*:*:*:*:*:*	CWE-284
CVE-2026-90436	Apache Axis 1.x (Through 1.4); N-able N-central (Including 2026.4.1.26 HF2)	cpe:2.3:a:apache:axis:*:*:*:*:*:*:*:*	CWE-470

Recommendations

Restrict Exposure and Disable the Legacy API: Put the N-central console and the "/dms" and "/dms2" SOAP services behind a VPN or zero-trust gateway rather than relying on IP allowlisting, because Agents, Probes and any compromised managed device can still reach them. 4EverAble2Shell needs the Legacy API, so confirm it is disabled on every on-premises server before the server returns to service, and keep it disabled until N-able ships a fix. Leave the Intune integration off until N-able confirms it is safe to restore.

Harden Agents and Accounts: Disable the Reactive ProcessController on Windows Agents where it isn't needed, and treat appliance IDs as sensitive, as they are the only prerequisite for Agent2Shell. Remove dormant, shared and over-privileged accounts (especially Technician and ProductAdmin) and enforce MFA for console logins.

Upgrade the Server, Agents and Probes: Upgrade on-premises servers to N-central 2026.4 HF2 (build 2026.4.1.26) through N-able's supported upgrade paths, and keep them offline until the upgrade is done. Then upgrade every Agent and then every Probe, because HF2 changes how they talk to the server. HF2 does not fix CVE-2026-90436 or Agent2Shell, so install N-able's promised follow-up hotfix as soon as it is released.

Hunt for Exploitation and Block Known Infrastructure: Search server logs for POSTs to "/dms/services/ServerUI" containing "jline.internal.TerminalLineSettings", DOCTYPE or external entities, or SessionID -1, and for RemoteExecutionTaskSubmit or ApplianceLogSubmit calls to "/dms2/services2/ServerMMS2". On the server, check for the flag_default.json symlink, serverchild- files, unexpected JSP files, the .xvd miner directories, xvd.service and cron entries tagged "# xvkeep". On Windows endpoints, look for encoded PowerShell running as SYSTEM and unexpected replacement of wsp.exe. Block 157[.]20[.]241[.]16, 5[.]231[.]45[.]175 and the two mining pools listed in the IoCs.

Treat Any Hit as Full Compromise: Isolate the affected server, preserve forensic images, and rebuild from a trusted baseline rather than cleaning in place. Rotate administrator passwords, API keys and Ecosystem Agent credentials. Remove unexpected administrator or Technician accounts, and assess every downstream customer network for follow-on activity.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1190: Exploit Public-Facing Application	
Execution	T1059: Command and Scripting Interpreter	T1059.004: Unix Shell
		T1059.006: Python
		T1059.001: PowerShell
Lateral Movement	T1072: Software Deployment Tools	
Persistence	T1505: Server Software Component	T1505.003: Web Shell
	T1543: Create or Modify System Process	T1543.002: Systemd Service
	T1053: Scheduled Task/Job	T1053.003: Cron
	T1098: Account Manipulation	
Privilege Escalation	T1068: Exploitation for Privilege Escalation	
	T1548: Abuse Elevation Control Mechanism	T1548.003: Sudo and Sudo Caching
Defense Evasion	T1140: Deobfuscate/Decode Files or Information	
	T1070: Indicator Removal	T1070.004: File Deletion
	T1564: Hide Artifacts	T1564.001: Hidden Files and Directories

Tactic	Technique	Sub-technique
Credential Access	T1552: Unsecured Credentials	T1552.001: Credentials In Files
Discovery	T1082: System Information Discovery	
Command and Control	T1105: Ingress Tool Transfer	
	T1095: Non-Application Layer Protocol	
	T1071: Application Layer Protocol	T1071.001: Web Protocols
Impact	T1496: Resource Hijacking	T1496.001: Compute Hijacking

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	157[.]20[.]241[.]16, 5[.]231[.]45[.]175, 3[.]74[.]48[.]121
IPv4:Port	157[.]20[.]241[.]16[:]8080, 139[.]99[.]69[.]109[:]10128, 79[.]76[.]51[.]56[:]39100, 5[.]231[.]45[.]175[:]8097
URL	hxxp[:]//157[.]20[.]241[.]16[:]8080/jup[.]sh, hxxp[:]//157[.]20[.]241[.]16[:]8080/xvgz, hxxp[:]//157[.]20[.]241[.]16[:]8080/xmrig[.]tgz, hxxp[:]//157[.]20[.]241[.]16[:]8080/ob/cronhit, hxxp[:]//157[.]20[.]241[.]16[:]8080/ob/fcheck, hxxp[:]//5[.]231[.]45[.]175[:]8097/a[.]dtd, hxxp[:]//5[.]231[.]45[.]175[:]8097/svc[.]xml
SHA256	fc4c01fd11bc301cf312830460cfdccc3af9dcfe50c910b86d6a1117bc76c747
Monero Address	41wx2Pv3FzfRvX11jQgzM4bRbgvr6GViRXCKkHhXhLVQ64mgUR5ks4CEzHx8zqUJ8MgsWwTaWiS3uiZbCgJQnNXoB19mGtr

Patch Link

https://me.n-able.com/s/softwaredownloads/a9jVy0000000LUHIA2/sd-000143

References

https://status.n-able.com/2026/11/10/n-central-2026-4-hf2-release-notes/

https://uptime.n-able.com/event/202609/

https://github.com/MSPNightmare/CVEs/tree/main/0-Days/N-Central%20N-Able

https://lists.apache.org/thread.html/8slf0j9gz35z56t0glt5h0ncwlbn4bdz

https://nvd.nist.gov/vuln/detail/CVE-2026-125883

https://nvd.nist.gov/vuln/detail/CVE-2026-90436

https://cyber.gc.ca/en/alerts-advisories/n-able-security-advisory-av26-1143

https://huntback.io/blog/ncentral-4everable2shell-miners-on-live-servers

https://blog.previdian.com/n-able-n-central-critical-vulnerabilities-what-we-know-so-far/

https://www.huntress.com/blog/n-able-disables-cloud-services-following-disclosure-of-able2shell-exploit-chains

https://labs.beazley.security/advisories/BSL-A1242

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a Demo of **HivePro**.

REPORT GENERATED ON

November 13, 2026 • 07:30 AM

© 2026 All Rights are Reserved by Hive Pro

More at www.hivepro.com