Indicators of Compromise (IOC) Summary

CVE-2026-90436 Confluence Exploitation & Downstream Incident

Prepared For	Legal Counsel (External Review)
Prepared By	CarltonOne Security Incident Response
Source Material	Rapid7 MDR Case 13257861 (case notes, analyst correspondence) and CarltonOne Security Incident Response Root Cause Analysis, v1.1 (Nov 17, 2026)
Related Vulnerability	CVE-2026-90436 — Unauthenticated RCE in Apache Axis 1.x (Confluence Remote API / SOAP-Axis1), a.k.a. CONFSERVER-104610
Document Purpose	Consolidated list of network, host, and infrastructure indicators associated with this incident, for legal review of notification and disclosure obligations
Date Prepared	November 18, 2026
Classification	Confidential — Privileged & Confidential, Prepared at the Request of Counsel

1. Purpose and Scope

This document consolidates the indicators of compromise (IOCs) identified during the investigation of a security incident affecting CarltonOne's Atlassian Confluence environment and related downstream systems. It is prepared to support legal review of potential notification obligations and is based on findings reported by Rapid7 Managed Detection and Response (MDR) and CarltonOne's internal Security Incident Response team.

This summary presents technical indicators only (IP addresses, domains, URLs, and related artifacts). It does not represent a final determination of the scope of data exposure, which is addressed separately in the full Root Cause Analysis and the associated data impact assessment. Several items noted below remain under investigation or pending confirmation, as indicated.

Important notes for reviewers:

- Some figures and attributions in the underlying source material are still being reconciled by Rapid7 and CarltonOne (for example, the method by which a Snowflake credential was obtained, and two differing estimates of weak password prevalence). Where this is the case, it is flagged in the relevant section.
- Defanged notation (e.g., hxxp, [.]) has been normalized to standard notation in this document for clarity and reference purposes. These indicators should not be entered into browsers or production systems.
- This is a living document. New indicators may be added as the investigation continues.

2. Incident Summary

Between approximately November 12, 2026, 10:08 PM EST and November 13, 2026, 1:54 PM EST, an external threat actor exploited an unauthenticated remote code execution vulnerability (CVE-2026-90436) affecting CarltonOne's internet-facing Atlassian Confluence server (util-atlassian-confluence, internal IP 10.98.98.212). Following initial access, the threat actor extracted credentials and sensitive content stored in the Confluence wiki, and used those credentials to access additional systems including Snowflake production data warehouses, SFTP file transfer servers, Jira, and Microsoft 365 accounts.

A related SQL injection campaign against a separate CarltonOne partner portal attributed to the same primary threat actor IP address was identified running concurrently and continuing for several days afterward.

The same threat actor IP address (192.238.253.176) is linked across all major phases of this activity. The last connection allowed through the perimeter firewall from any identified threat actor IP occurred on November 15, 2026 at 5:01 AM EST; blocked connection attempts continued through November 16, 2026.

3. IP Address Indicators

3.1 Primary Threat Actor IP Address

The following IP address is assessed with high confidence as the primary threat actor address, observed across nearly every phase of the incident: initial reconnaissance, exploitation, credential harvesting, SFTP access, Microsoft 365 sign-ins, and the related SQL injection campaign.

IP Address	First Observed	Associated Activity
192.238.253.176	Nov 12, 2026 ~11:30 PM UTC	Initial reconnaissance, RCE exploitation support, credential harvesting, 174 successful SFTP logins, M365/SharePoint access (94% of ~98,000 requests)

3.2 Additional Confirmed Threat Actor IP Addresses

IP Address	Associated Activity
5.133.47.243	Identified by Rapid7 as threat actor infrastructure; blocked at firewall
163.182.68.109	Identified by Rapid7 as threat actor infrastructure; blocked at firewall; additional denied connection attempts logged post-containment
104.13.106.166	Identified by Rapid7 as threat actor infrastructure; blocked at firewall
71.217.68.146	Targeted M365 account of a C1 Employee following Confluence containment
47.201.228.15	M365/Graph sign-in activity; connected to internal address 70.33.230.125:443; allowed through firewall on Nov 15 prior to blocking
65.27.15.41	M365/Graph sign-in activity associated with compromised mulesoft@carltonone.com account
73.141.163.144	M365 sign-in activity (hubspot-automation-test account); allowed through firewall on Nov 15 prior to blocking

3.3 Exploitation-Phase Source IPs (Examples)

The exploitation phase against the Confluence Remote API endpoint involved a large pool of rotating source addresses (424+ distinct IPs, 1,835 total requests), consistent with use of a residential proxy network. The addresses below are specific examples called out in the investigation; the full address list is retained in the underlying Confluence access logs and has not been reproduced in full here.

IP Address	Role
47.218.187.29	First request to vulnerable SOAP/Axis endpoint
98.162.66.115	Retrieved service WSDL definition from vulnerable endpoint
71.58.37.211	Source of the request associated with confirmed RCE (shell spawned, id command exfiltrated)
173.40.168.11	Example proxy IP within the 424-address exploitation pool
172.56.29.151	Example proxy IP within the 424-address exploitation pool
184.60.185.18	Example proxy IP within the 424-address exploitation pool

3.4 Shared / Third-Party Infrastructure (Do Not Block)

The following IP addresses belong to Cloudflare's shared tunnel infrastructure (trycloudflare.com) and were used as C2/exfiltration relay points. Because this infrastructure is shared across many legitimate Cloudflare customers, these addresses are listed for log-search and monitoring purposes only and are not recommended for blocking.

IP Address	Context
`104.16.231.132`	Cloudflare address contacted by the compromised Confluence host, and separately by util-openmetadata and admintools.grsportal.com
`104.16.230.132`	Additional Cloudflare address associated with trycloudflare.com tunnel activity in this incident

4. Domain and Tunnel-Service Indicators

The threat actor used multiple public webhook and tunneling services to stage payloads, receive command output, and exfiltrate data, rotating between services to blend malicious traffic with legitimate cloud service usage.

4.1 Webhook / Notification Services

Domain	Purpose
`webhook.site`	RCE verification callback and exfiltration of configuration files, directory listings, and system enumeration data
`ntfy.sh`	C2 notification channel

4.2 Cloudflare Tunnel Subdomains (*.trycloudflare.com)

The following subdomains were observed hosting payloads or receiving exfiltrated data. Each resolves to shared Cloudflare tunnel infrastructure and is unique to this threat actor's tunnel session.

Subdomain	Known Role
`performer-created-shaped-pros.trycloudflare.com`	Hosted Snowflake exfiltration script (i9754_sfexec.py)
`oscar-grew-think-entirely.trycloudflare.com`	Contacted by util-openmetadata (10.98.98.242)
`bend-standard-patch-prepare.trycloudflare.com`	Exfiltration of Kerberos/AS-REP attack artifacts
`regression-rats-finding-contrary.trycloudflare.com`	Associated threat actor tunnel
`forward-favour-aids-web.trycloudflare.com`	Associated threat actor tunnel
`critics-char-glass-corresponding.trycloudflare.com`	Associated threat actor tunnel

Cloudflare tunnel subdomains, continued:

Subdomain	Known Role
dinner-afterwards-penn-boolean.trycloudflare.com	Associated threat actor tunnel
consisting-collectibles-founder-motion.trycloudflare.com	Associated threat actor tunnel
royal-brick-butler-pregnant.trycloudflare.com	Associated threat actor tunnel
warriors-app-hopes-answered.trycloudflare.com	Associated threat actor tunnel
bits-jersey-showed-deals.trycloudflare.com	Associated threat actor tunnel
extended-park-prepared-stage.trycloudflare.com	Associated threat actor tunnel

4.3 Pinggy Tunnel Domains

Domain	Known Role
wpefh-192-238-253-176.free.pinggy.net	Hosted exfiltration script (i8110h.sh); received exfiltrated content of 6 targeted Confluence wiki pages
aruwe-192-238-253-176.free.pinggy.net	Additional tunnel subdomain associated with the same threat actor
lin.us.5.a.pinggy.click	Additional tunnel domain identified in later analysis
lin.us.13.a.pinggy.click	Additional tunnel domain identified in later analysis
zoqii-192-238-253-176.run.pinggy-free.link	Additional tunnel domain identified in later analysis

5. Specific URLs / Exfiltration Endpoints

The following specific URLs (paths and parameters) were identified in command execution and network logs as destinations for data exfiltration or payload retrieval. Shown here in standard (non-defanged) notation for reference.

URL	Data Transmitted / Purpose
webhook.site/0c973170-b6d6-47e1-81cc-baac66d65368?stage=rce1&d=...	Base64-encoded output of the 'id' command (RCE verification)
webhook.site/0c973170-b6d6-47e1-81cc-baac66d65368?t=cfg_orig	Confluence configuration file containing plaintext MySQL database password
webhook.site/0c973170-b6d6-47e1-81cc-baac66d65368?t=dirs	Enumerated directory and file listing
webhook.site/70defd43-cc46-4039-bff3-6714535190c8?t=fp2	Internal service fingerprint and port scan results
wpefh-192-238-253-176.free.pinggy.net/raw?f=i8110h.sh	Delivery of payload script used to query the Confluence database directly
wpefh-192-238-253-176.free.pinggy.net/post?t=i8110h	Exfiltration of 6 targeted Confluence wiki pages
performer-created-shaped-pros.trycloudflare.com/raw?f=i9754_sfexec.py	Delivery of Snowflake query/exfiltration script
bend-standard-patch-prepare.trycloudflare.com/up?t=asreq_all.log	Exfiltration of Kerberos AS-REP roasting attempt log
/plugins/servlet/soap-axis1/confluenceservice-v2	Exploited endpoint — unauthenticated legacy Confluence SOAP/Axis service (CVE-2026-90436)

6. Vulnerability Reference

Identifier	Description
CVE-2026-90436	Unauthenticated remote code execution in Apache Axis 1.x, bundled within Atlassian Confluence Data Center (versions 1.x–9.x). Reachable only when the legacy Confluence Remote API (XML-RPC & SOAP) feature is enabled. Also tracked by Atlassian as CONFSERVER-104610. This is the confirmed root-cause vulnerability for this incident.

7. Associated Tools and Host Artifacts

The following tool names and file artifacts were identified on affected systems during the investigation and may assist in scanning for related activity elsewhere in the environment.

Artifact	Context
`i8110h.sh`	Shell script executed in memory; queried the Confluence database directly using the harvested MySQL password
`i9754_sfexec.py`	Script used to query Snowflake production data using stolen OPENMETADATA_SVC credentials
`i8431_p3.py`	Associated script artifact
`/tmp/i9646_agent.sh, i9699_agent.sh, i9700_agent.sh, i9755_agent.sh`	Reverse-shell / persistence agent scripts identified running on the compromised host
`Python HTTP listener, port 19001`	Exfiltration listener process found running on the compromised host (logged to /tmp/i9755_exfil.log)
`Impacket — GetNPUsers.py`	Used for AS-REP roasting against Active Directory (Kerberos pre-authentication abuse), staged in /tmp/pylibs
`Impacket — GetTGT.py`	Used to request a Kerberos Ticket Granting Ticket using a harvested credential
`sqlmap 1.10.11`	Automated SQL injection tool used against one partner's portal
`/tmp/users.txt, /tmp/cand2.txt`	Wordlist and 25-account target list used for credential attacks against Active Directory
`/tmp/asreq_all.log, asrep_all.txt, asrep_cand.txt`	Kerberos attack output files, subsequently exfiltrated

8. Affected Systems and Accounts (Summary)

A detailed accounting of affected systems, accounts, and data categories is maintained in the full Root Cause Analysis and the separate data impact assessment. At a summary level, the investigation confirmed threat actor access to or use of:

- The Confluence application server and its underlying database (util-atlassian-confluence)
- Snowflake production data warehouses (DB_P2MPROD and DB_GRSPROD), accessed using a compromised service account credential (OPENMETADATA_SVC)
- 23 SFTP accounts across three file transfer servers, using credentials harvested from Confluence
- Microsoft 365 accounts: mulesoft@carltonone.com and a service account, hubspot-automation-test@carltonone.com
- Jira, accessed via 33 named accounts over a 12-hour period
- A single partner portal via SQL injection, attributed to the same primary threat actor IP

This document does not itself characterize the volume or categories of personal information involved; that assessment is addressed in the data impact review referenced in the Root Cause Analysis (Section 4.4) and is being finalized separately.

9. Current Containment Status

- All primary and additional threat actor IP addresses listed in Section 3 have been blocked at the perimeter firewall.
- The compromised Confluence host has been quarantined and preserved for forensic purposes; it has not been returned to production.
- The last connection from a known threat actor IP allowed through the firewall occurred November 15, 2026, 5:01 AM EST (10:01 UTC).
- Blocked connection attempts from threat actor infrastructure continued through November 16, 2026, 12:38 AM EST (05:38 UTC); none have been observed since that time as of the date of this document.
- Credential rotation for affected accounts (SFTP, Snowflake service account, M365 accounts, targeted Active Directory accounts) is in progress; completion status for each should be confirmed against the Root Cause Analysis corrective actions tracker (Section 5.1) before this document is finalized for external use.

10. Document Status and Caveats

This is a working summary and remains subject to change as the investigation continues.

• Several attribution and scope questions remain open with Rapid7 as of this document's preparation date, including the precise source of the compromised Snowflake credential and reconciliation of two different estimates of weak password prevalence on one partner’s portal.

• IP addresses, domains, and tools listed reflect confirmed or strongly indicated threat actor infrastructure as assessed by Rapid7 and CarltonOne's internal response team. Some exploitation-phase proxy addresses (Section 3.3) are drawn from a larger pool (424+ addresses) and are illustrative rather than exhaustive.

• This document should be read together with the full Root Cause Analysis report for complete context on timeline, scope of impact, and remediation status.