January 13, 2025

Cyberattack on BeyondTrust Exposes Security Vulnerabilities

Overview: BeyondTrust, a leading Privileged Access Management (PAM) company, faced a significant cyberattack in early December 2024. The breach targeted its Remote Support SaaS instances, exposing vulnerabilities in its infrastructure and impacting a limited number of customers. The attack highlights the ongoing risks associated with secure remote access solutions used by critical sectors such as government, healthcare, energy, and banking. The incident began on December 2, 2024, when anomalous behavior was detected on the company's network. A subsequent investigation revealed that attackers had gained access to an API key, enabling them to reset passwords for local application accounts on compromised Remote Support SaaS instances. BeyondTrust took immediate action by revoking the compromised API key, notifying affected customers, and providing alternative support instances.

CTI Analysis: During the post-attack investigation, BeyondTrust identified two critical vulnerabilities within their Remote Support (RS) and Privileged Remote Access (PRA) products:

- **CVE-2024-12356 (CVSS score 9.8**): A critical command injection vulnerability which allows unauthenticated remote attackers to execute operating system commands within the context of the site user.
- **CVE-2024-12686 (CVSS score 6.6)**: A medium-severity vulnerability which allows attackers with administrative privileges to inject commands and upload malicious files to the target system.

Although BeyondTrust's advisories do not confirm active exploitation of these flaws during the attack, CISA has reported that CVE-2024-12356 was exploited in subsequent attacks. It remains unclear if the vulnerabilities were zero-day exploits used to breach BeyondTrust systems or downstream customers.

Updated forensic findings indicate that the attackers leveraged a compromised API key to gain initial access, resetting local application account passwords. BeyondTrust's timeline reveals proactive measures, including patches for both cloud and self-hosted instances and forensic investigations in collaboration with third-party cybersecurity firms. The updates as

of January 6, 2025, confirm that all SaaS instances are fully patched, with no further affected customers identified.

Impact Analysis: The breach impacted a limited number of customers, raising concerns about the potential downstream effects on organizations relying on BeyondTrust's Remote Support SaaS. The vulnerabilities (particularly CVE-2024-12356) could enable attackers to compromise secure access environments, steal sensitive data, or inject malicious code. However, BeyondTrust clarified that there is no evidence of ransomware deployment linked to the breach. The incident's broader implications include weakened security for organizations relying on compromised SaaS instances, intensifying scrutiny over PAM solutions and their vulnerability management protocols, and an increased risk of exploitation in environments where critical patches remain unapplied.

Indicators of Compromise (IoCs)

IPv4 Addresses	IPv6 Addresses
147[.]182[.]207[.]218	2604[:]a880:400:d1::7293:c001
165[.]232[.]151[.]16	2604[:]a880:400:d1::72ad:3001
143[.]110[.]235[.]149	2604[:]a880:400:d1::7716:1
167[.]71[.]24[.]236	2604[:]a880:400:d1::7df0:7001
162[.]243[.]173[.]155	2604[:]a880:400:d1::8622:f001
146[.]190[.]169[.]165	2604[:]a880:400:d1::1000:3001
157[.]230[.]183[.]1	2604[:]a880:400:d1::6721:1001
192[.]81[.]209[.]168	2604[:]a880:400:d1::6ce6:3001
24[.]144[.]114[.]85	2604[:]a880:400:d1::40a7:f001
142[.]93[.]119[.]175	2604[:]a880:400:d1::44dd:a001
23[.]95[.]182[.]25	2604[:]a880:400:d1::7035:8001
138[.]197[.]88[.]50	2400[:]6180:10:200::727:0
206[.]189[.]189[.]107	2604[:]a880:4:1d0::17e7:7000
94[.]158[.]247[.]83	2604[:]a880:4:1d0::d2e:8000
5[.]181[.]159[.]96	2604[:]a880:400:d1::6e64:e001
67[.]217[.]228[.]191	2604[:]a880:400:d1::5321:6001
5[.]181[.]159[.]16	2604[:]a880:400:d1::545e:4001
64[.]227[.]17[.]214	2604[:]a880:400:d1::6e00:f001
64[.]227[.]17[.]241	2604[:]a880:400:d1::7123:8001

Mitigations:

BeyondTrust has implemented the following measures to address the incident and associated vulnerabilities:

- Immediate deactivation of the compromised API key and suspension of impacted SaaS instances.
- Automatic updates applied to all cloud instances to address CVE-2024-12356 and CVE-2024-12686. Self-hosted instance users must manually apply security updates.
- Continuous communication and updates provided to affected customers.

Organizations using BeyondTrust solutions are advised to:

1. Ensure immediate application of all security patches for both cloud and self-hosted instances.
2. Conduct internal audits to assess potential compromise.
3. Strengthen monitoring for anomalous activities related to PAM and remote access systems.

Conclusion: The cyberattack on BeyondTrust underscores the critical importance of securing privileged access and remote support solutions. While the company's swift response mitigated immediate risks, the incident highlights the ongoing challenges in safeguarding complex infrastructures against evolving threats. Organizations must prioritize proactive vulnerability management and implement robust monitoring practices to minimize risks associated with privileged access.

Source:

https://www.dmnews.com/beyondtrust-reports-cyberattack-on-remote-support-saas/

https://censys.com/cve-2024-12356/

https://www.bleepingcomputer.com/news/security/beyondtrust-says-hackers-breached-remote-support-saas-instances/

https://www.beyondtrust.com/remote-support-saas-service-security-investigation