Radware breach exposes some customers' Cloud WAF log-export credentials



Radware says an unauthenticated internal Cloud WAF management API was reachable from the internet, exposing customer contact details and, for some, log-export credentials for AWS S3, Azure Blob Storage or SFTP. Affected customers should rotate keys.

- On 19 November 2026 an unauthorized party accessed an internal Cloud WAF management API that required no authentication and was reachable from the public internet.
- Potentially accessed data: customer contact details and, for a subset of customers, log-export credentials for AWS S3, Azure Blob Storage or SFTP.
- Radware reports no exposure of WAF traffic inspection, certificates, end-user data, application traffic or cloud DDoS services.
- Some customers have reported AWS alerts about an unfamiliar IP address trying to reach their log-

export buckets; the investigation continues.

- Radware strongly advises affected AppSec (WAF, BOT) customers to rotate credentials and review storage access logs from at least 19 November.

Radware has disclosed that attackers reached an internal Cloud WAF management API that was exposed to the public internet without authentication. According to the company's root cause analysis, as reported by BleepingComputer, the unauthorized access took place on 19 November 2026 and was detected about ten hours later.

What was exposed

Radware says the information potentially accessed includes customer contact details and, for a subset of customers, the credentials configured to export logs into self-managed storage: AWS S3, Azure Blob Storage or SFTP. The company states that WAF traffic inspection, certificates, end-user data, customer application traffic and cloud DDoS services and data were not exposed, and that it has found no evidence of changes to customer security policies.

The investigation is ongoing. Radware is still determining whether exposed keys were used without authorization, and some customers have already reported AWS alerts about an unfamiliar IP address attempting to access their log-export buckets.

Response so far

Radware blocked the originating IP address and access to the API, and revoked and replaced all internal account credentials. It strongly advises affected AppSec (WAF, BOT) customers to rotate Cloud WAF log-export credentials as soon as possible and to review storage access logs for unexpected activity since at least 19 November. At the time of reporting, the company had not issued a public statement.

Why it matters

Log-export credentials grant access to storage that may hold request logs. Institutions that use Cloud WAF with their own storage should treat the keys as potentially compromised until verified otherwise, and confirm whether contractual notification duties apply.

What to do now

1. Confirm whether your organisation uses Radware Cloud WAF with log export to AWS S3, Azure Blob Storage or SFTP, and contact Radware to learn whether you are affected.
2. Rotate the log-export credentials now: AWS access keys, Azure storage keys or SAS tokens, and SFTP credentials.
3. Review access logs on the log-export storage accounts from 19 November 2026 onward for unfamiliar IP

addresses or unexpected reads.

4. Restrict the exported-log storage with least-privilege permissions and source IP allow-listing where feasible.
5. If unauthorized access is found, activate incident response and assess notification duties to NCA, SAMA or SDAIA under applicable requirements and contracts.
6. Add third-party credential exposure scenarios to your supplier risk reviews.