Rapid Patch & Defense Checklist

F5 Breach Response

Immediate actions

- ☐ **Patch Immediately** - *Apply F5's October 2025 security updates across all BIG-IP, BIG-IQ, and F5OS devices. Verify patch version numbers and check for any missed systems through automated inventory.*

- ☐ **Lock Down Management Access** - Disable public exposure of management interfaces.
  - Move admin access behind VPN or zero-trust gateway
  - Enforce MFA
  - Restrict by IP allowlist

- ☐ **Retire End-of-Support Devices** – Outdated gear = soft targets.
  - ☐ Identify EoS hardware
  - ☐ Replace or isolate within segmented network

- ☐ **Rotate Credentials and API Keys** – Change passwords, SSH keys, service accounts, and API tokens tied to F5 devices. Use a secrets vault to track and audit rotations.

- ☐ **Verify Software Integrity** - F5 rotated its signing certificates post-incident.
  - Validate firmware signatures and checksums
  - Download updates only from official MyF5 portal
  - Document verification in change logs

- ☐ **Turn Up Visibility** – Monitor everything related to management and traffic control planes.
  - Send BIG-IP logs to SIEM
  - Alert on new admin users, config edits, or data spikes
  - Hunt weekly for anomalies or Brickstorm-related indicators

Disclaimer

The materials, documents, and tools shared by Point Break Security GmbH and The Daily Signal channel are provided free of charge for the purpose of supporting and educating our audience.

While every effort is made to ensure accuracy and usefulness, Point Break Security GmbH, The Daily Signal, and any individual involved in producing or distributing this content do not guarantee the quality, accuracy, or suitability of the information or materials provided.

We cannot be held responsible or liable for any damages, losses, or issues that may arise from the use, misuse, or interpretation of these materials.

Users are solely responsible for verifying that any scripts, configurations, or recommendations are compatible with their own environment and for thoroughly testing them in a controlled or non-production setting before applying them to live systems.

By using these materials, you acknowledge that you do so at your own risk and accept full responsibility for how they are implemented.