F5 BIG-IP Privilege Escalation and BIG-IQ Vulnerability

Overview

F5 has released patches addressing a critical privilege escalation vulnerability in BIG-IP and a medium-severity cross-site scripting (XSS) vulnerability in BIG-IQ. The vulnerabilities, tracked as CVE-2024-45844 (BIG-IP) and CVE-2024-47139 (BIG-IQ), could allow attackers to gain unauthorized system access and compromise affected appliances.

CVE-2024-45844/BIG-IP (CVSS 8.6) is a privilege escalation vulnerability in the appliance's monitor functionality, allowing authenticated attackers with Manager role or higher to elevate privileges and make configuration changes. There is no exposure to the data plane; this flaw only affects the control plane. Affected Versions: BIG-IP versions 17.1.1, 16.1.4, and 15.1.10

CVE-2024-47139/BIG-IQ (CVSS 4.8) is a stored XSS vulnerability that can be exploited by an attacker with administrator privileges to execute malicious JavaScript within the BIG-IQ user interface. Affected Versions: BIG-IQ centralized management versions prior to 8.2.0.1 and 8.3.0

Researchers have confirmed that there is a published PoC for CVE-2024-45844. Due to this, Aspire recommends patching the systems as soon as possible.

Aspire Protects

- **Patch –** Organizations using the affected versions of BIG-IP and BIG-IQ are urged to apply the latest patches:
  - 17.1.1.4, 16.1.5, 15.1.10.5 for BIG-IP. Find patch guidance in F5's Knowledge Base Article.
  - 8.2.0.1, 8.3.0 for BIG-IQ. Find patch guidance in F5's Knowledge Base Article.
- Ensure that only trusted users with the Manager role or higher have access to critical systems.

IoCs

There are no known IoCs associated with the above vulnerabilities at this time. Aspire is actively monitoring and will notify customers if any are found. For more details on how we can help protect your organization, contact Aspire's Customer Success Management team.

TTPs to Watch

CVE-2024-45844

- **Initial Access**
  - Exploit Public-Facing Application (T1190) - Attackers may leverage CVE-2024-45844 by exploiting the BIG-IP monitor functionality to elevate privileges and modify configurations after gaining authenticated access.

- **Privilege Escalation**
    - Abuse Elevation Control Mechanism (T1548.002) - Authenticated attackers with Manager role or higher can exploit CVE-2024-45844 to elevate their privileges, gaining unauthorized control over BIG-IP systems.
- **Impact**
    - Data Manipulation (T1565.001) - Attackers exploiting either CVE-2024-45844 or CVE-2024-47139 can manipulate system or user data, either by modifying system configurations or executing unauthorized JavaScript.
- **Collection**
    - Input Capture - Credential API Hooking (T1056.004): Malicious scripts injected into the BIG-IQ interface could be used to capture input, such as administrator credentials, giving attackers further access to sensitive systems.

Aspire Service Offerings

- **Aspire Managed XDR (MXDR)**
    - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.
    - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors. Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyberattacks.
- **Aspire Incident Response**
    - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.
    - Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

Supporting Documentation

CVE-2024-45844: Privilege escalation in F5 BIG-IP - Almond Offensive Security Blog

Article Detail (f5.com)