ICT DIVISION
FUTURE IS HERE

BANGLADESH COMPUTER COUNCIL
COMPUTER FOR EVERYTHING

BGD e-GOV CIRT

TLP:CLEAR

Active Exploitation of Critical F5 BIG - IP Vulnerability (CVE–2023-46747) Uncovered in Bangladesh

[This page is intentionally left blank]

TLP: CLEAR
Distribution: Public
Type of Threat: RCE Vulnerability (CVE-2023-46747)
Date: 06 November 2024

Executive Summary

The Cyber Threat Intelligence Unit of the Bangladesh e-GOV Computer Incident Response Team (BGD e-GOV CIRT) has uncovered active evidence of compromise associated with a critical vulnerability in F5 BIG-IP systems, widely used across Bangladesh's IT infrastructure. The investigation revealed that attackers managed to gain shell access on a compromised system and later attempted to sell this unauthorized access on a dark web marketplace. On October 30, a threat actor claimed to have root-level access to a server, initially offering it for a set price, which was later increased to $2,500 on November 4.

Further analysis confirmed the presence of CVE-2023-46747, a severe authentication bypass vulnerability that allows attackers to execute remote code without authentication, enabling access to the Traffic Management User Interface (TMUI) on F5 BIG-IP systems. This vulnerability, which can grant attackers full administrative control, has also been exploited in combination with CVE-2023-46748, a high-severity SQL injection flaw observed in active attacks reported by F5.

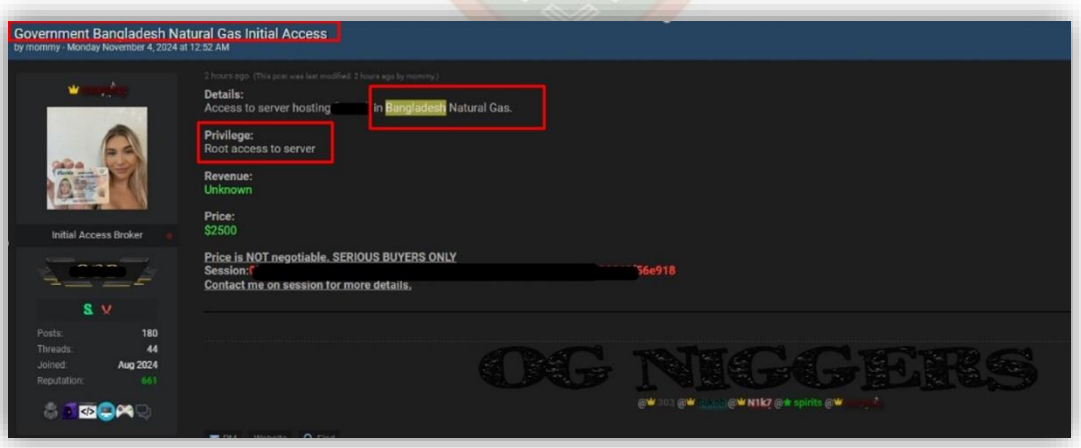

Figure: TA repost the access offer and raising the price for 2500$

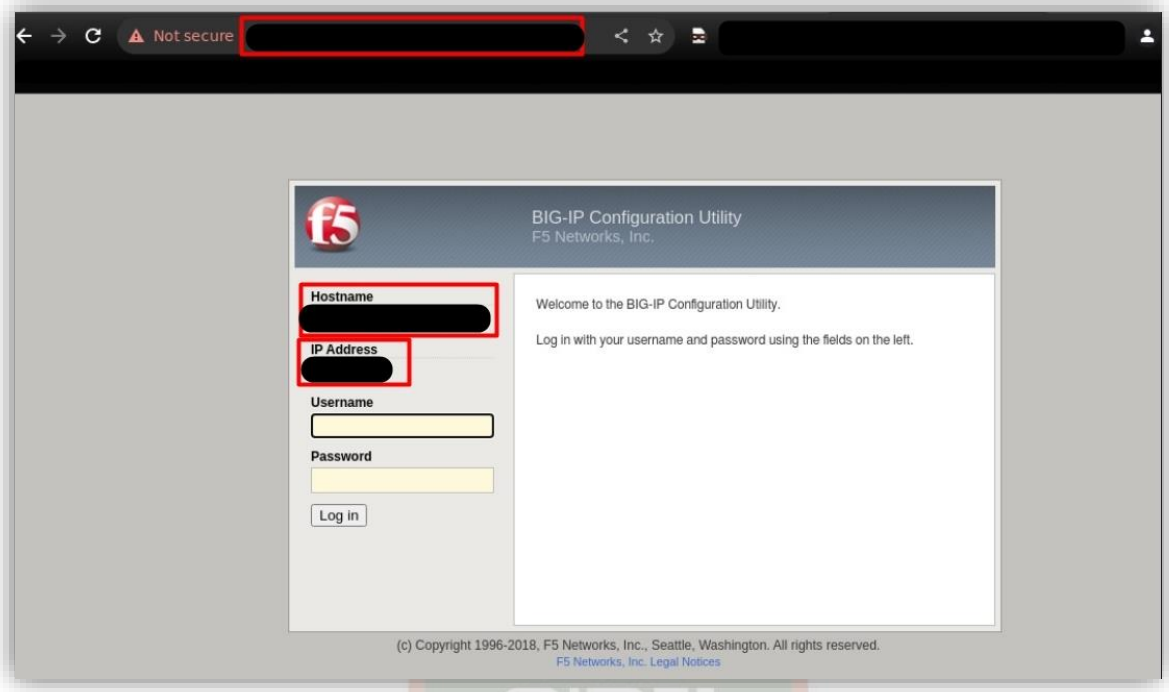

Figure: Login portal of the victim asset claimed by the threat actor

Importance of Responsible Disclosure

Our Cyber Threat Intelligence Unit at BGD e-GOV CIRT promptly notified the appropriate management teams about the compromise and conducted a thorough investigation, identifying the compromised server's IP address, hostname, and F5 BIG-IP web interface link. To support immediate containment, we provided swift mitigation steps to assist with further investigation and recovery efforts.

We recommend contacting affected organizations first before disclosing breach details to the public. Premature disclosures can cause unwanted dread, especially if the actual threats, attack vectors and impact are different from what is reported. Such disclosures can also alert threat actors, allowing them to avoid detection and continue their activities. Responsible disclosure builds trust in the cybersecurity community, strengthens defenses, and helps protect organizations and users, contributing to a safer digital environment for all.

CVE-2023-46747 vulnerability overview:

On October 25, 2023, cybersecurity firm Praetorian[1] disclosed CVE-2023-46747, a critical vulnerability in F5 BIG-IP systems' Traffic Management User Interface (TMUI). This flaw, with a CVSSv3 score of 9.8, enables unauthenticated attackers to gain full administrative access and execute remote code due to improper input validation. On October 26, F5 confirmed the vulnerability, also detailing CVE-2023-46748, a high-severity SQL injection flaw (CVSSv3 8.8) that has been observed in active exploit chains with CVE-2023-46747, further increasing the risk to affected systems.

Category	Count
Identified Systems in Bangladesh with CVE-2023-46747	2
Active F5 Systems Identified via Internet Scan in Bangladesh	168

Impact:

The successful exploitation of CVE-2023-46747 poses significant risks to F5 BIG-IP systems, leading to severe consequences for affected organizations. Key impacts include:

- **Unauthorized System Access:** Attackers may gain privileged access to critical systems, allowing for data manipulation and further attacks.
- **Arbitrary Code Execution:** Malicious actors could execute arbitrary code on compromised devices, resulting in unauthorized actions and system control.
- **Service Disruption and Data Exposure:** Exploitation may lead to service interruptions and the exposure of sensitive information, risking data breaches and loss of trust.
- **Lateral Movement Potential:** Attackers may move laterally across connected systems, compromising broader network infrastructure and leading to widespread damage.

Affected Versions:

CVE-2023-46747 affects F5 BIG-IP systems operating under the following conditions:

- **BIG-IP Versions Prior to 17.0**: All versions preceding 17.0 are vulnerable.
- **Exposed Management Interfaces**: Deployments with publicly accessible management interfaces, particularly those lacking strict access controls or IP restrictions, are at heightened risk.

Note: Organizations should consult F5's official documentation[2] for comprehensive details on affected versions and recommended remediation steps.

[1] https://www.praetorian.com/blog/advisory-f5-big-ip-rce/
[2] https://my.f5.com/manage/s/article/K000137353

Potential signs of intrusion:

In the context of CVE-2023-46747, the following indicators may signify potential exploitation of F5 BIG-IP devices. Proactive monitoring for these signs is essential for timely detection and response:

- **Unauthorized Logins:** Monitor for irregular login activity on the BIG-IP management interfaces, including logins from unusual IP addresses and multiple failed attempts, especially outside standard operational hours.
- **Suspicious Network Traffic:** Be vigilant for unusual API calls or traffic directed at F5 BIG-IP endpoints. Look for patterns such as excessive requests, unexpected HTTP methods, or significant traffic **spikes.**
- **Unauthorized Configuration Changes:** Watch for unanticipated modifications to configurations on BIG-IP devices, especially those made without proper authorization or outside scheduled maintenance periods.
- **Increased Resource Usage:** Regularly check for spikes in CPU or memory usage on affected systems. Unexplained increases may indicate targeting or compromise.

Mitigation and Recommendations:

To mitigate the risks associated with CVE-2023-46747, organizations using F5 BIG-IP systems should implement the following measures:

1. **Patch Deployment**: Apply the latest security patches released by F5 to address this vulnerability.
2. **Restrict Access:** Limit access to the F5 BIG-IP management interface to internal IPs only, reducing public exposure.
3. **Implement Multi-Factor Authentication (MFA):** Enforce MFA for all users accessing the BIG-IP management portal to enhance security.
4. **Enhanced Logging and Monitoring**: Enable comprehensive logging on BIG-IP systems and monitor for anomalous activity, particularly concerning privileged actions.
5. **Isolate Compromised Systems:** Immediately isolate any systems showing signs of compromise and conduct a thorough investigation.

Conclusion

This advisory emphasizes the critical nature of CVE-2023-46747, especially for organizations operating within Bangladesh. Immediate patching, access control reinforcement, and proactive monitoring are vital to mitigating this risk. BGD e-GOV CIRT remains committed to supporting national infrastructure security and preventing unauthorized exploitation of this vulnerability.