KPMG Cyber Threat Intelligence Platform

Remote Takeover of F5's Big-IP

F5 disclosed a critical remote code execution vulnerability tracked under CVE-2022-1388 on 4 May 2022, which allows exploiting implementation flaws in BIG-IP system's management interface, much like its predecessor CVE-2020-5902. The vulnerability allows an unauthenticated adversary to bypass the authentication mechanism and gain root privileges. The vulnerability affects multiple versions of the network management interface of F5's BIG-IP systems, and basis the gathered open-source intelligence, it is estimated that around 16000 BIG-IP systems are on public facing internet, which are at the risk from attackers.

The vulnerability emerges from a faulty authentication in the web-based management interface. The REST API component of F5's BIG IP modules - iControl, is impacted with authentication bypass vulnerability. Since its disclosure, organizations are being mass scanned for potentially exposed management port of BIG IP appliances and several proof-of-concepts are already being circulated throughout the internet. Attackers are keen on using this as an initial attack vector to gain access of the system and leverage it for further infiltration into the victim's network. Once compromised, threat actors might drop web shells to gain backdoor access or install malware on the system.

Given the criticality and triviality of the issue, organizations are urged to assess their infrastructure for the vulnerability and upgrade to the latest software version as suggested by F5. Further it is advised to take down the management interface over the public internet in order to mitigate this vulnerability.

What should you do?

- Monitor Indicators of Compromise (IoCs) in your environment to identify anomalies.
- Ensure your Windows environment is patched to the brim and is protected with multi-factor authentication.
- Conduct a comprehensive, full spectrum, threat assessment exercise to uncover blind spots and improvement areas.

The KPMG Cyber Threat Intelligence Platform is an industry defining, research-based capability for enhanced visibility into cyber threats.

Our machine ingestible feeds and analysis are the result of automated, sensor-based intelligence metrics with dedicated, expert insights of each threat to provide you the appropriate context on a timely basis in industry standard formats such as STIX/ TAXII/ MISP.

These feeds are additionally co-related with our industry partners and independent research for additional context. The intelligence obtained is then curated from strategic, tactical and operational perspective to give you a wide-ranging view of cyber threats.

We also assist you with our renowned cyber incident response and threat hunting services in case you identify an active threat in your environment.

We offer a wide-range of services, including:
Strategic threat intelligence report
Machine ingestible threat intelligence feeds
Threat intelligence driven pre-emptive threat hunting exercise
Cyber Incident Response Services

Contact us:

KPMG in India Cyber Response Hotline : +91 9176 471 471

Atul Gupta
Partner, Head of Cyber Security,
KPMG in India
T: +91 98100 81050
E: atulgupta@kpmg.com

B V, Raghavendra
Partner, KPMG in India
T: +91 98455 45202
E: raghavendrabv@kpmg.com

Sony Anthony
Partner, KPMG in India
T: +91 98455 65222
E: santhony@kpmg.com

Chandra Prakash
Partner, KPMG in India
T: +91 99000 20190
E: chandraprakash@kpmg.com

Manish Tembhurkar
Associate Partner,
KPMG in India
T: +91 98181 99432
E: mtembhurkar@kpmg.com

KPMG

KPMG Cyber Threat Intelligence Platform

Remote Takeover of F5's Big-IP

Indicators of Compromise: IP Addresses	
81.69.58[.]15	178.23.190[.]52
64.39.98[.]40	212.102.50[.]210
77.91.72[.]39	209.58.170[.]164
217.252.7[.]13	196.65.108[.]171
208.71.210[.]1	154.23.191[.]157
66.94.126[.]14	85.106.114[.]175
64.39.98[.]227	202.28.229[.]174
64.39.98[.]196	68.183.202[.]236
64.39.98[.]159	66.254.159[.]252
64.39.98[.]152	193.178.210[.]87
146.19.75[.]41	223.187.119[.]114
223.72.39[.]119	204.195.115[.]184
210.92.18[.]153	198.252.101[.]110
139.99.149[.]66	198.211.120[.]110
69.24.129[.]229	216.162.206[.]213
77.91.101[.]249	209.127.252[.]207
194.156.98[.]67	202.103.212[.]140
194.156.98[.]43	

Indicators of Compromise: Domains	
nishabii[.]live	dota[.]uiasuibasdbui[.]art
uiasuibasdbui[.]art	dota[.]iwishiwashappy[.]eu
iwishiwashappy[.]eu	dota[.]zzzsleepisnicezzz[.]art
zzzsleepisnicezzz[.]art	

Indicators of Compromise: Hashes
27c44dd2edc626df03504ce129f5c021
a824640862ea34979abb4d80f2ee07b1
752c413cd4949d285acc9b9f23685e73
d4586ea75fd99c224ae768839295012c
d22be45c7d7efefc8bf8a2ba4c5c71ab
c3464dd8e01ceb676b342be2022fc826
9856920aeba17304e35a620e64390d40
b659aecf1ea18b82018d44b401f9252a

KPMG

KPMG Cyber Threat Intelligence Platform

Remote Takeover of F5's Big-IP

Indicators of Compromise: Hashes
7c99389e6f1af3f883eb2484c287369a
4d37d0410931c64d123e60033ef3db25
b659aecf1ea18b82018d44b401f9252a
6784fe2d6da666f1bfbb2c3d388da999
61eec0a0f4bc84bfcb16e86f60e96e6f
4e55f1c3630f86edb695b20734270d20
05dec77dbc765b43d3b969146da92bb6
966af57a4e9fdf5e81be6bb5d830691d
95ce67dde417001c9091a3f2dfeac8e9
79c0b8d26490a27029d5af0487853f90
5c568df5fdd4d61ab57e178b0a357203
587f440ac6f584e0e0da03bfa6afb51e
1b335ade9f990f28d9561f94bec1aa75
12fad047124e504881bfeefe7706edb2
F58140b6d73da382dc9867732cb8a2f0c46d1287
E0983b5b4c158c78c1c55089627d744b6ac424d8
D643d3ef5b64cd91d99286c04924c8dd1de3d315
Bfb1fea2fcacf615c8c8921f5cded10fafb84529
24a7022009444d5dce70514e854e424527b47f90
8e5eb65e10d4bfac532b368be841abba57f3e62b
F58140b6d73da382dc9867732cb8a2f0c46d1287
72097d4e8145f4b341c7d8df9754c33cee90edd5
529fbd21cf1eb8cdbd5cbc9c59c074cebd8262ed
D1b6d156bc6042c0deaafe7f5b0b7ebed313e69b
E4aa390460c2e7132f104d15b3e85aeb50dfc164
95f01c6e2c4468f29295155dad06cc1e2c4c2364
9344ec7eb4d1dcc6db69cf473aceaafcf471dd2f
8e5eb65e10d4bfac532b368be841abba57f3e62b
8bfdcd018924e5a67d0383853194ac4ca0ac8598
791a40cae572aa17ea62763dc130fdacb0eeac21
73732f3bd90ffc768f24c15bb1df4a6aeea17702
5ca0bb0abcde0d22b78054936aed8f519a51f44a
5b87cc7500d77cd7ffdf1ad251c47ccc91879731
5a4070dc5b5bea8e2529424b944bc832e4bf2edf

KPMG

KPMG Cyber Threat Intelligence Platform

Remote Takeover of F5's Big-IP

Indicators of Compromise: Hashes
168d8f3d3748761c8cc5ceaf9e7fad1f5b5ad02a
398614898be6e5c07e2aaf4f22d3ac37209238ee
eb9e5466833c3a5e771e917491fea0bea2f3af2d
C6a9d06cbb4124abd398548710f14f318ccf2c09
5111b0f913f50a2902f719d6782e16f770dd0dbe74e2d121bb3fd0c052556664
316d5fe2d8e263fbff5bff510036b592b83cb18bc0e08ab6442f79e2b3eb87c1
07ce9028bfd638d778e5cbae6acb1a4ff3657d10f44c69b8af93bd1175736ec3
2195137730783a83cbedc8d72a84296c9cbab6e169338d7951677ddbc6555d7f
82c8bd3bd715892bbc09625c9bf3b1f27ddab81f6cbcc974b526c700b31cd755
8888449dc9796981ca363c0fb9b1e877fe045902ade45966f4037af8eea3d198
8f5a1d760ebc4cbcce7851dbef8802b83d2c30a56797ae101b649abb959eed12
Aaa4aaa14e351350fccbda72d442995a65bd1bb8281d97d1153401e31365a3e9
Ca15a055b2e1d06a8fbd3a22341aeda29bbc19688b778dc3a15c615f0367bc21
30f7e1998d162dfad69d6d8abb763ae4033bbd4a015d170b1ad3e20d39cd4e20
Da647646cd36a3acb716b4266e9032f9c1caf555b7667e1dbe5bef89e7d2fdbb
B39d2a1202351d3be5d9906ec47ee05c305302124dddec5538dc7b9924c6b85d
Ad6d44c70f83431bedf890967f2da0607c9b1f79591fb1b2697160f5b1c1a75c
1f93a6696f7bf1b2067cc503583deb4840404ebeeba89579bd303f57000baeb7
9a72aab2a3d1d6e66c185966597a52a8726ca25f5d9e2195af44f98d8b1847d5
53214f4d2d2dfd02b46f416cbdcb6f3a764820a50da4d59926f829b96cf82a6c
Be45cb2a9d6d030f12824051d66a90269453a7eff885734e15835839eef39226
E088177f26fbeb8f60b7915d2bb9bd6dd5bbeb99c88ccef23cafc3d96d1a83d8
9d7f6dca67fcb9147a7f974861ea9f4e8fce2d87b159c43da44bcb466a658831
9c59376168b04f16dd2bbdd4e8748848b3329f2278c273bc45ce8e9d8d1ad3aa
782e08725417e6bdb6f521c61bc5798bf4952e16d586cf9faf87be9de17e607a
72fe93e9570560f581f6564b265418c6a9a92851602adbfaeb07517cc4858fee
5f1d50dea3eeb2f951420c3ec469a38661bbf5e044b676aedebf734832da1e9a
9197691b1e0dd5e8aa8c8d7dd14e34ad34c8deb36fa44fd1791827546bd700e2
ab7ffbac9230a375b22baf9e5aa0e76d4f368fd609deff6ec4d1cec6aa255e16