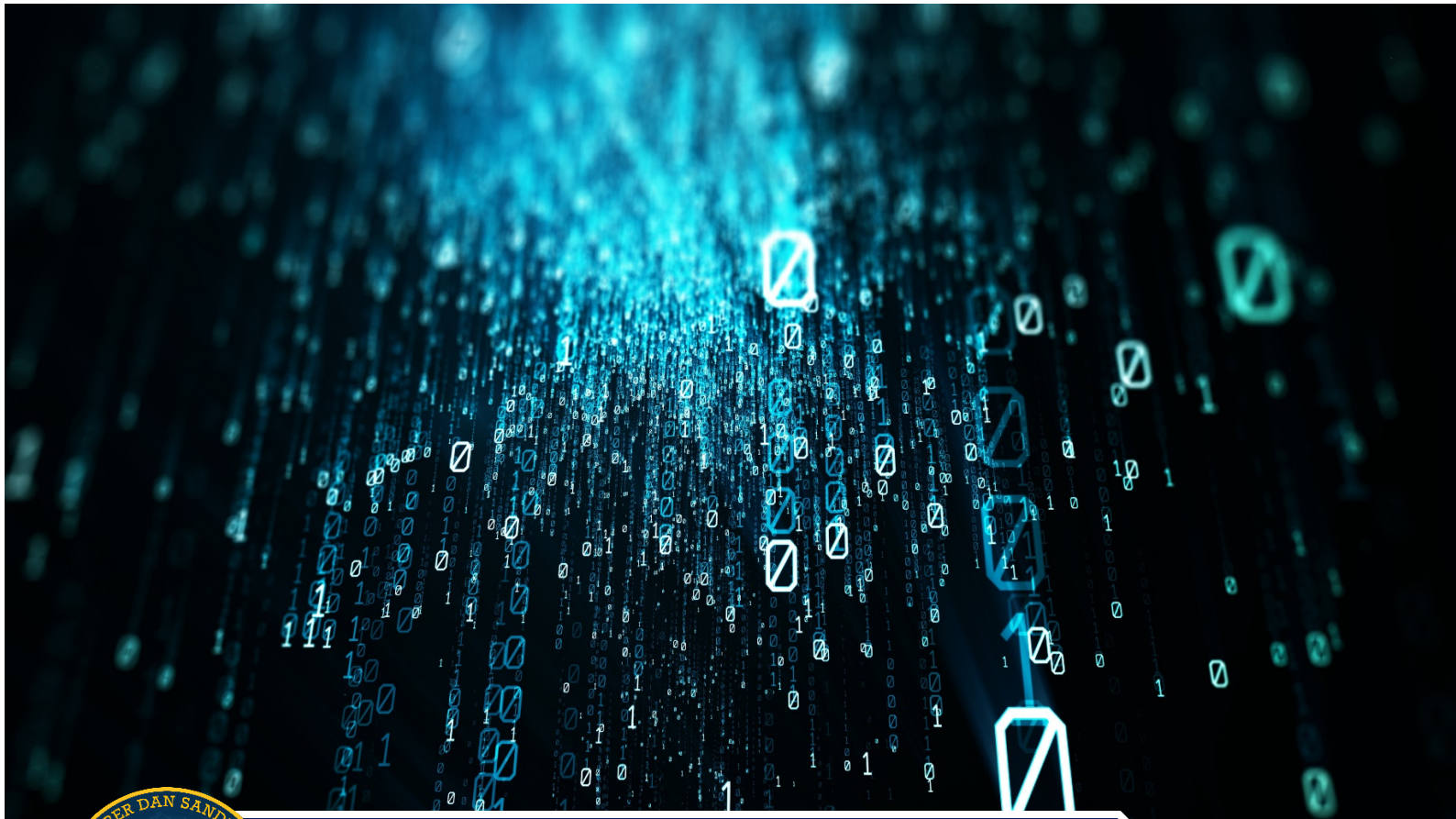


DIREKTORAT PROTEKSI INFRASTUKTUR INFORMASI KRITIKAL NASIONAL

DEPUTI BIDANG PROTEKSI

IMBAUAN KEAMANAN

CVE-2021-23008: Kerentanan Otentikasi pada BIG-IP *Access Policy Manager Active Directory*

TLP:WHITE

PENDAHULUAN

Pada tanggal 28 April 2021, F5 mempublikasikan sebuah *security advisory* (K51213246) [1] mengenai kerentanan otentikasi pada BIG-IP *Access Policy Manager* (APM) *Active Directory* (AD). Berikut deskripsi kerentanan CVE-2021-23008.

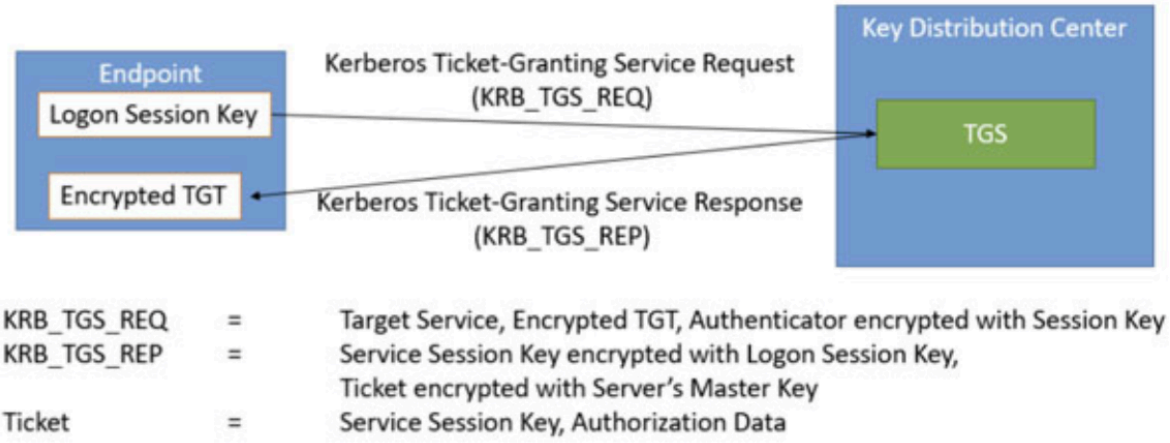
CVE	*Description*	*Privileges*	CVSSv3.1 *Score*
CVE-2021-23008	F5 BIG-IP APM AD *authentication vulnerability*	*Unauthenticated*	**8.1 Critical** 3.1#CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

Peneliti mengungkapkan kerentanan *bypass* pada fitur keamanan *Key Distribution Center* (KDC) yang berdampak pada layanan pengiriman pada aplikasi F5 BIG-IP. Kerentanan spoofing pada KDC memungkinkan penyerang untuk melakukan *bypass* otentikasi Kerberos ke BIG-IP *Access Policy Manager* (APM) [2].

ANALISIS

CVE-2021-23008 merupakan kerentanan *authentication bypass* yang bersifat kritikal yang ditemukan pada BIG-IP *Access Policy Manager* (APM) *Active Directory* (AD). Kerentanan ini memiliki skor **CVSSv3.1 8.1** dengan tingkat ***severity High***. Kerentanan memungkinkan penyerang untuk melakukan *bypass* otentikasi Kerberos ke BIG-IP *Access Policy Manager*. Pada beberapa kasus, kerentanan juga dapat digunakan untuk melakukan *bypass* otentikasi ke *console* admin BIG-IP.

Kerberos merupakan protokol otentikasi *client-server* dengan mutual authentication dan membutuhkan perantara terpercaya yang disebut sebagai *Key Distribution Center* (KDC) - Server otentikasi Kerberos atau Server ticketing yang bertindak sebagai tempat penyimpanan kunci semua pengguna serta informasi hak akse pengguna [2]. Proses otentikasi Kerberos dapat dilihat pada Gambar 1.



Gambar 1. Proses Otentikasi pada Kerberos.

Salah satu aspek yang juga penting adalah otentikasi KDC ke server. Tidak adanya keamanan pada Kerberos akan memungkinkan penyerang untuk melakukan *hijacking* ke dalam jaringan antara BIG-IP dan *domain controller*. Jika Kerberos diimplementasikan dengan benar, maka penyerang tidak akan dapat melakukan *bypass* otentikasi. Penyerang dapat melakukan *hijack* pada koneksi KDC menggunakan *spoofed AS-REP response*.

APM Access policy diatur dengan otentikasi *active directory* dan *single sign on* (SSO). Jika kredensial palsu terkait kerentanan ini digunakan, tergantung pada *back end sytem* memvalidasi token otentikasi yang diterima, kemungkinan besar akses akan gagal. *APM Access policy* juga dapat mengatur otentikasi sistem BIG-IP. Penggunaan kredensial palsu pada *administrative user* melalui APM *Access Policy* akan menghasilkan akses lokal.

Sistem terdampak

F5 *Product Development* telah mempublikasikan sistem yang terdampak kerentanan ini, sebagai berikut [1][4].

Produk	Versi	Versi yang Rentan	*Patch*	*Severity*	*CVSS Score*	Komponen/ Fitur yang Rentan
BIG-IP APM	16.x	16.0.0 - 16.0.1	None	High	8.1	APM AD *auth*
	15.X	15.0.0 - 15.1.2	15.1.3			
	14.x		14.1.4			
	13.x		13.1.4			
	12.x		12.1.6			
	11.x		*None*			
BIG-IP(LTM, AAM, AFM, Analytic, ASM, DNS, FPS, GTM, Link Controller, PEM)	16.x	*None*				
	15.X	*None*	*Not applicable*	*Not Vulnerable*	*None*	*None*
	14.x	*None*	*Not applicable*			
	13.x	*None*	*Not applicable*			
	12.x	*None*	*Not applicable*			
	11.x	*None*	*Not applicable*			
BIG-IQ Centralized Management	7.x	*None*	*Not applicable*	*Not Vulnerable*	*None*	*None*
	6.x	*None*	*Not applicable*	*Not Vulnerable*	*None*	*None*
	5.x	*None*	*Not applicable*	*Not Vulnerable*	*None*	*None*
Traffix SDC	5.x	*None*	*Not applicable*	*Not Vulnerable*	*None*	*None*

Distribusi pengguna produk BIG-IP di Indonesia

Berikut data pengguna produk BIG-IP *Access Policy Manager Active Directory* di Indonesia berdasarkan informasi yang didapat dari *opensource intelligence:*

KOTA:

Jakarta	63
Bandung	5
Semarang	5
Surabaya	4
Bireun	2

PROOF OF CONCEPT (PoC)

Sampai dengan dokumen ini dibuat belum ditemukan *proof of concept* (PoC) dan *exploit script* untuk kerentanan CVE-2021-23008.

Namun, Silverfort menjelaskan tahapan yang dapat dilakukan penyerang untuk memalsukan KDC untuk *bypass* otentikasi dengan asumsi mampu melakukan *hijacking* komunikasi jaringan antara BIG-IP dan KDC. Serangan dilakukan dengan *redirecting traffic* antara BIG-IP dan KDC (*domain controller*) pada port 88 (port Kerberos) ke Windows Server Silverfort. Terdapat domain palsu pada windows server dan memastikan terdapat *user ID* yang sama dengan administrator BIG-IP pada domain sebenarnya. *Password* yang digunakan adalah '1' pada *fake domain*. Kemudian dilakukan loggin pada *traffic* yang dialihkan ke KDC palsu, *password* '1' akan berfungsi.

LANGKAH MITIGASI DAN PENANGANAN KERENTANAN

Jika masih menggunakan BIG-IP APM AD dengan versi yang rentan, kerentanan dapat dihilangkan dengan melakukan pembaruan ke dalam versi yang telah di rilis *patch*-nya. Jika tidak menemukan versi yang dimiiki, maka belum terdapat pemutakhiran untuk versi tersebut.

Sangat disarankan bagi pengguna BIG-IP APM AD untuk memeriksa pembaruan *advisory* pada situs F5 *Network*.

Langkah - Langkah Mitigasi

Untuk memitigasi kerentanan, dapat dilakukan langkah-langkah berikut [1][3]:

1. Menerapkan konfigurasi *multi-factor authentication*, atau menerapkan *host-level authentication* seperti dengan mengembangkan *IPSec tunnel* antara sistem BIG-IP APM yang terdampak dengan server *Active Directory.* Administrator juga harus melakukan monitoring terhadap Kerberos secara terus menerus untuk menemukan anomali, yaitu *resource* yang hanya mengirimkan *request* AS_REQ, tanpa TGS _REQ.
2. *APM Access policy* diatur dengan otentikasi *active directory* dan *single sign on* (SSO). Jika kredensial palsu terkait kerentanan ini digunakan, tergantung pada *back end sytem* memvalidasi token otentikasi yang diterima, kemungkinan besar akses akan gagal. *APM Access policy* juga dapat mengatur otentikasi sistem BIG-IP. Penggunaan kredensial palsu pada *administrative user* melalui APM *Access Policy* akan menghasilkan akses lokal.
3. Jika sistem otentikasi BIG-IP menggunakan otentikasi *active directory*, maka dapat digunakan otentikasi secara remote dari *User Directory* yang memiliki pilihan otentikasi dengan SSL. *Key configuration* memungkinkan “SSL Option” dan mengkonfigurasinya sesuai dengan kebutuhan otentikasi *remote* yang akan digunakan: *Active Directory*, LDAP, dan *ClientCert* LDAP.
4. Admin melakukan validasi bahwa implementasi Kerberos memerlukan *password*/*keytab*. Untuk melakukan validasi perlu digunakan beberapa *shared secret.* Jika tidak memungkinkan melakukan konfigurasi *file keytab* atau *password* akun, maka aplikasi rentan terhadap *spoofing* KDC.

Catatan:

Ketika mengimplementasikan *patch* keamanan yang nantinya akan di rilis, tidak akan berdampak negarif pada sistem.

- Informasi mengenai ***Configuring IPSec between a BIG-IP and Third-Party device*** terdapat dalam **BIG-IP TMOS: *Tunnelling and IPSec Guide*,** dapat

diakses pada link https://techdocs.f5.com/en-us/bigip-14-1-0/big-ip-tmos-tunneling-and-ipsec-14-1-0.html.

- Informasi mengenai ***Configuring Remote User Authentication and Authorization*** terdapat dalam **BIG-IP TMOS: *Implementation Guide*,** dapat diakses pada link https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/tmos-implementations-13-0-0.html

Limitasi

- Belum dirilis pembaruan (*update) patch* untuk versi 16.x.

REFERENSI

[1] F5, "K51213246: BIG-IP APM AD authentication vulnerability CVE-2021-23008," 28 April 2021. [Online]. Available: https://support.f5.com/csp/article/K51213246, diakses 5 Mei 2021.

[2] The Hacker News, "F5 BIG-IP Found Vulnerable to Kerberos KDC Spoofing Vulnerability". 28 April 2021 .[Online]. Available: https://thehackernews.com/2021/04/f5-big-ip-found-vulnerable-to-kerberos.html, diakses 5 Mei 2021.

[3] Threatpost, "F5 BIG-IP Vulnerable to Security-Bypass-Bug ". 29 April 2021. [Online]. Available: https://threatpost.com/f5-big-ip-security-bypass/165735/, diakses 5 Mei 2021.

[4] Auscert, "BIG-IP APM: Multiple vulnerabilities (ESB-2021.1450)". 29 April 2021.[Online]. Available: https://www.auscert.org.au/bulletins/ESB-2021.1450, diakses 5 Mei 2021.