Aditinet-pre-packed

Fixed cost peace of mind for your investment

Installation | Health-check | **Upgrade** | Migration | Skills transfer | Custom

Speed up engagement by working faster and smarter with our pre-packed service options.

The recent vulnerability exposed by F5, CVE-2020-5902, has forced companies to rapidly upgrade their F5 environments due to vulnerability receiving a severity score of 10 from CVSS. At Aditinet we'd like to not only inform you of the circumstances under which you may be vulnerable and the potential ramifications but also offer a packaged service that aims to resolve it in an efficient and cost-effective manner.

This is the reference from F5: https://support.f5.com/csp/article/K52145254

This vulnerability allows for unauthenticated attackers, or authenticated users, with network access to the Configuration utility, through the BIG-IP management port and/or self IPs, to execute arbitrary system commands, create or delete files, disable services, and/or execute arbitrary Java code. This vulnerability may result in complete system compromise. The BIG-IP system in Appliance mode is also vulnerable. This issue is not exposed on the data plane; only the control plane is affected.

This table highlights the affected versions:

Product	Branch	Versions known to be vulnerable	Fixes introduced in	Severity	CVSSv3 score[1]	Vulnerable component or feature
BIG-IP (LTM, AAM, Advanced WAF, AFM, Analytics, APM, ASM, DDHD, DNS, FPS, GTM, Link Controller, PEM, SSLO)	16.x	None	16.0.0	Not vulnerable	None	None
	15.x	15.0.0 - 15.1.0	15.1.0.4‡	Critical	10.0	TMUI/Configuration utility
	14.x	14.1.0 - 14.1.2	14.1.2.6			
	13.x	13.1.0 - 13.1.3	13.1.3.4†			
	12.x	12.1.0 - 12.1.5	12.1.5.2			
	11.x	11.6.1 - 11.6.5	11.6.5.2			
BIG-IQ Centralized Management	7.x	None	Not applicable	Not vulnerable	None	None
	6.x	None	Not applicable			
	5.x	None	Not applicable			
Traffix SDC	5.x	None	Not applicable	Not vulnerable	None	None

The simplest and most effective way to resolve the vulnerability is to perform an upgrade of the TMOS software running on the appliances.

The standard time to complete of an F5 appliance or cluster software upgrade are displayed below, in most scenarios the work is prepared during an “In hours” window whilst the upgrade occurs in an “Out of hours” window, the breakdown of the standard scenarios are displayed below.

Description of F5 Environment	In hours work	Out of hours work
Standalone F5	1 day	½ day
High Availability Pair	1 day	½ day

These can be scaled to any customer environment by assessing the number of instances of Standalone and High Availability pairs of F5 appliances that require the upgrade and multiply by the respective timings.

The standard upgrade to resolve the vulnerability will include a move to the most up-to-date version of the current major version of running software, e.g. 11.6.1 → 11.6.5.2 or 13.1.0 → 13.1.3.4 etc. Discussions to move to a higher major version of TMOS are available on request.

Contact your supplier partner now to arrange a scoping call and book your upgrade.

Contact us on https://aditinet.uk/contact-us