EFOS 3.4.4.3 OpenSSH and OpenSSL Vulnerabilities

CVE-ID	Impact	Summary	Status
Not Vulnerable to all CVE issues prior to CVE-2017-15906			
CVE-2017-15906	Medium	Allows attackers to create zero-length files.	Fixed in EFOS 3.4.4.2 and subsequent releases
CVE-2018-0734	Medium	The OpenSSL DSA signature algorithm has been shown to be vulnerable to a timing side channel attack.	Fixed in EFOS 3.4.4.2 and subsequent releases
CVE-2018-15473	Medium	User enumeration vulnerability due to not delaying bailout for an invalid authenticating user	Fixed in EFOS 3.4.4.2 and subsequent releases
CVE-2018-15919	Medium	Could allow remote attackers to detect existence of users on a target system when GSS2 is in use	Fixed in EFOS 3.4.4.2 and subsequent releases
CVE-2018-5407	Medium	Simultaneous Multi-threading (SMT) in processors can enable local users to exploit software vulnerable to timing attacks via a side-channel timing attack on 'port contention	Fixed in EFOS 3.4.4.2 and subsequent releases
CVE-2019-1559	Medium	If an application encounters a fatal protocol error at shutdown the user may be provided with a padding oracle that could be used to decrypt data	Fixed in EFOS 3.4.4.2 and subsequent releases
CVE-2020-3120	Medium	Cisco CDP on Cisco FXOS Cisco IOS XR and Cisco NX-OS. Vulnerability to a stack overflow in the parsing of PortID type-length-value(TLV)	1) Checks have been added to validate this field/value with number of addresses that EFOS supports. 2) Added extra validation to ensure that the value in 'Number of addresses' field is in sync with length value in the received TLV.