Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Application					
Antiy					
Anti Virus Lab Atool					
DoS Exec Code Overflow	2018-12-22	7.2	Local attackers can trigger a Kernel Pool Buffer Overflow in Antiy AVL ATool v1.0.0.22. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. The specific flaw exists within the processing of IOCTL 0x80002004 by the ssdt.sys kernel driver. The bug is caused by failure to properly validate the length of the user-supplied data. An attacker can leverage this vulnerability to execute arbitrary code in the context of the kernel, which could lead to privilege escalation. A failed exploit could lead to denial of service. **CVE ID : CVE-2018-20331**	N/A	A-ANT-ANTI-030119/1
Audiocoding					
Freeware Advanced Audio Decoder 2					
N/A	2018-12-22	4.3	A NULL pointer dereference was discovered in ifilter_bank of libfaad/filtbank.c in Freeware Advanced Audio Decoder 2 (FAAD2) 2.8.8. The vulnerability causes a	N/A	A-AUD-FREE-030119/2

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			segmentation fault and application crash because adding to windowed output is mishandled in the EIGHT_SHORT_SEQUENCE case. **CVE ID : CVE-2018-20362**		
DoS Overflow	2018-12-22	4.3	An invalid memory address dereference was discovered in the hf_assembly function of libfaad/sbr_hfadj.c in Freeware Advanced Audio Decoder 2 (FAAD2) 2.8.8. The vulnerability causes a segmentation fault and application crash, which leads to denial of service. **CVE ID : CVE-2018-20361**	N/A	A-AUD-FREE-030119/3
DoS Overflow	2018-12-22	4.3	An invalid memory address dereference was discovered in the sbr_process_channel function of libfaad/sbr_dec.c in Freeware Advanced Audio Decoder 2 (FAAD2) 2.8.8. The vulnerability causes a segmentation fault and application crash, which leads to denial of service. **CVE ID : CVE-2018-20360**	N/A	A-AUD-FREE-030119/4
DoS Overflow	2018-12-22	4.3	An invalid memory address dereference was discovered in the sbrDecodeSingleFramePS function of libfaad/sbr_dec.c in Freeware Advanced Audio Decoder 2 (FAAD2) 2.8.8. The vulnerability causes a segmentation fault and	N/A	A-AUD-FREE-030119/5

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			application crash, which leads to denial of service. **CVE ID : CVE-2018-20359**		
DoS Overflow	2018-12-22	4.3	An invalid memory address dereference was discovered in the lt_prediction function of libfaad/lt_predict.c in Freeware Advanced Audio Decoder 2 (FAAD2) 2.8.8. The vulnerability causes a segmentation fault and application crash, which leads to denial of service. **CVE ID : CVE-2018-20358**	N/A	A-AUD-FREE-030119/6
N/A	2018-12-22	4.3	A NULL pointer dereference was discovered in sbr_process_channel of libfaad/sbr_dec.c in Freeware Advanced Audio Decoder 2 (FAAD2) 2.8.8. The vulnerability causes a segmentation fault and application crash. **CVE ID : CVE-2018-20357**	N/A	A-AUD-FREE-030119/7
DoS	2018-12-17	4.3	A NULL pointer dereference was discovered in ifilter_bank of libfaad/filtbank.c in Freeware Advanced Audio Decoder 2 (FAAD2) 2.8.8. The vulnerability causes a segmentation fault and application crash, which leads to denial of service because adding to windowed output is mishandled in the ONLY_LONG_SEQUENCE case.	N/A	A-AUD-FREE-030119/8

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2018-20199		
DoS	2018-12-17	4.3	A NULL pointer dereference was discovered in ifilter_bank of libfaad/filtbank.c in Freeware Advanced Audio Decoder 2 (FAAD2) 2.8.8. The vulnerability causes a segmentation fault and application crash, which leads to denial of service because adding to windowed output is mishandled in the LONG_START_SEQUENCE case. **CVE ID : CVE-2018-20198**	N/A	A-AUD-FREE-030119/9
DoS	2018-12-17	4.3	A NULL pointer dereference was discovered in ic_predict of libfaad/ic_predict.c in Freeware Advanced Audio Decoder 2 (FAAD2) 2.8.8. The vulnerability causes a segmentation fault and application crash, which leads to denial of service. **CVE ID : CVE-2018-20195**	N/A	A-AUD-FREE-030119/10
Frogcms Project					
Frogcms					
XSS	2018-12-25	3.5	Frog CMS 0.9.5 has XSS via the Database name field to the /install/index.php URI. **CVE ID : CVE-2018-20448**	N/A	A-FRO-FROG-030119/11
Radare					
Radare2					
N/A	2018-12-25	4.3	In radare2 prior to 3.1.1, core_anal_bytes in libr/core/cmd_anal.c allows	N/A	A-RAD-RADA-030119/12

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attackers to cause a denial-of-service (application crash caused by out-of-bounds read) by crafting a binary file. **CVE ID : CVE-2018-20461**		
Overflow	2018-12-25	4.3	In radare2 prior to 3.1.2, the parseOperands function in libr/asm/arch/arm/armass64.c allows attackers to cause a denial-of-service (application crash caused by stack-based buffer overflow) by crafting an input file. **CVE ID : CVE-2018-20460**	N/A	A-RAD-RADA-030119/13
N/A	2018-12-25	4.3	In radare2 prior to 3.1.1, r_bin_dyldcache_extract in libr/bin/format/mach0/dyldcache.c may allow attackers to cause a denial-of-service (application crash caused by out-of-bounds read) by crafting an input file. **CVE ID : CVE-2018-20458**	N/A	A-RAD-RADA-030119/14
DoS	2018-12-25	4.3	In radare2 prior to 3.1.1, the parseOperand function inside libr/asm/p/asm_x86_nz.c may allow attackers to cause a denial of service (application crash in libr/util/strbuf.c via a stack-based buffer over-read) by crafting an input file, a related issue to CVE-2018-20455. **CVE ID : CVE-2018-20456**	N/A	A-RAD-RADA-030119/15
DoS Overflow	2018-12-25	4.3	In radare2 prior to 3.1.1, the parseOperand function inside	N/A	A-RAD-RADA-030119/16

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			libr/asm/p/asm_x86_nz.c may allow attackers to cause a denial of service (application crash via a stack-based buffer overflow) by crafting an input file, a related issue to CVE-2018-20456. **CVE ID : CVE-2018-20455**		
Sass-lang					
Libsass					
DoS	2018-12-17	4.3	In LibSass 3.5.5, a NULL Pointer Dereference in the function Sass::Eval::operator()(Sass::Supports_Operator*) in eval.cpp may cause a Denial of Service (application crash) via a crafted sass input file. **CVE ID : CVE-2018-20190**	N/A	A-SAS-LIBS-030119/17
S-cms					
S-cms					
Sql	2018-12-25	7.5	An issue was discovered in S-CMS 1.0. It allows SQL Injection via the js/pic.php P_id parameter. **CVE ID : CVE-2018-20480**	N/A	A-SCM-SCMS-030119/18
Sql	2018-12-25	7.5	An issue was discovered in S-CMS 1.0. It allows SQL Injection via the wap_index.php?type=newsinfo S_id parameter. **CVE ID : CVE-2018-20479**	N/A	A-SCM-SCMS-030119/19
Sql	2018-12-25	7.5	An issue was discovered in S-CMS 3.0. It allows SQL Injection via the	N/A	A-SCM-SCMS-030119/20

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			bank/callback1.php P_no field. **CVE ID : CVE-2018-20477**		
XSS	2018-12-25	4.3	An issue was discovered in S-CMS 3.0. It allows XSS via the admin/demo.php T_id parameter. **CVE ID : CVE-2018-20476**	N/A	A-SCM-SCMS-030119/21
OS					
Orange					
Arv7519rw22 Livebox 2.1 Firmware					
N/A	2018-12-23	10	Orange Livebox 00.96.320S devices allow remote attackers to discover Wi-Fi credentials via /get_getnetworkconf.cgi on port 8080, leading to full control if the admin password equals the Wi-Fi password or has the default admin value. This is related to Firmware 01.11.2017-11:43:44, Boot v0.70.03, Modem 5.4.1.10.1.1A, Hardware 02, and Arcadyan ARV7519RW22-A-L T VR9 1.2. **CVE ID : CVE-2018-20377**	N/A	O-ORA-ARVL-030119/22
Schneider-electric					
Modicom Bmxnor0200h Firmware; Modicom M340 Firmware; Modicom Premium Firmware; Modicom Quantum Firmware					
+Info	2018-12-17	5	An Information Exposure through Discrepancy vulnerability exists in the embedded web servers in all Modicon M340, Premium, Quantum PLCs and BMXNOR0200 where the web	https://www.schneider-electric.com/en/download/document/	O-SCH-MODI -030119/23

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			server sends different responses in a way that exposes security-relevant information about the state of the product, such as whether a particular operation was successful or not. **CVE ID : CVE-2018-7812**	SEVD-2018-327-01/	
N/A	2018-12-17	5	An Improper Check for Unusual or Exceptional Conditions vulnerability exists in the embedded web servers in all Modicon M340, Premium, Quantum PLCs and BMXNOR0200 where an unauthenticated user can send a specially crafted XML data via a POST request to cause the web server to become unavailable **CVE ID : CVE-2018-7833**	https://www.schneider-electric.com/en/download/document/SEVD-2018-327-01/	O-SCH-MODI-030119/24
N/A	2018-12-17	5.8	A URL Redirection to Untrusted Site vulnerability exists in the embedded web servers in all Modicon M340, Premium, Quantum PLCs and BMXNOR0200 where a user clicking on a specially crafted link can be redirected to a URL of the attacker's choosing. **CVE ID : CVE-2018-7804**	https://www.schneider-electric.com/en/download/document/SEVD-2018-327-01/	O-SCH-MODI-030119/25