Anhang

Tab. A.1 Softwareumfänge in technischen Systemen [Chip2014] mit Fehlerraten nach eigener Berechnung

Software-Anwendung	Codeumfang	Fehler Standard 0,5% (V-Modell)	Fehler Höchstqualität: 0,01% (Militär, Aerospace)
Durchschnittliche iPhone-App	40.000	200	4
Herzschrittmacher	80.000	400	8
Photoshop 1.0	128.000	640	13
Space-Shuttle-Software	400.000	2.000	40
Grafikschnittstelle CryEngine 2	1.000.000	5.000	100
Hubble-Weltraumteleskop	2.000.000	10.000	200
Windows 3.1	2.500.000	12.500	250
Kontrollsoftware einer US-Militärdrohne	3.500.000	17.500	350
Mars Curiosity Rover	5.000.000	25.000	500
Google Chrome	7.000.000	35.000	700
Photoshop CS 6	10.000.000	50.000	1.000
OpelAmpera	10.000.000	50.000	1.000
Android OS	12.000.000	60.000	1.200
Boeing 787 Dreamliner	14.000.000	70.000	1.400
Linux3.10	16.000.000	80.000	1.600
Firefox Browser	18.000.000	90.000	1.800
F-35 Kampfflugzeug	24.000.000	120.000	2.400
Windows7	40.000.000	200.000	4.000
Microsoft Office 2013	45.000.000	225.000	4.500
Teilchenbeschleuniger Large Hadron Collider	50.000.000	250.000	5.000
Windows Vista	50.000.000	250.000	5.000
Facebook	62.000.000	310.000	6.200
MacOSXI0.4	86.000.000	430.000	8.600
Steuersoftware für moderne Autos	100.000.000	500.000	10.000
Webseite healthcare.gov	500.000.000	2.500.000	50.000
Menschliches Genom	3.300.000.000	16.500.000	330.000

Die folgenden Tab. (A.1, A.2) stellen Auszüge aus den wöchentlichen Meldungen des US-CERT bzw. ICS-CERT mit höchster Kritikalität dar. Sie zeigen insbesondere, dass die Entwicklung der Anzahl der aufgedeckten Schwachstellen sich nicht vermindert. Neben den genannten Herstellern oder Produkten gilt dies nahezu für alle Hersteller und Produkte. Die Schwachstellen sind systematischer Natur und werden in der letzten Spalte klassifiziert. Es ist zu erkennen, dass eine typstrenge Sprache wie Ada die meisten der hier genannten Schwachstellen prinzipiell vermeidet.

H. B. Keller, *Entwicklung von Echtzeitsystemen*,
https://doi.org/10.1007/978-3-658-26641-7

Tab. A.2 Schwachstellen in existierenden Systemen (siehe [US2016])

Datum	Software	Text	Ursache
Cisco - Auszug (294 Schwachstellen gefunden innerhalb 1 Jahr)			
28.02.2019	cisco -- rv110w_firmware	A vulnerability in the web-based management interface of the Cisco RV110W Wireless-N VPN Firewall, Cisco RV130W Wireless-N Multifunction VPN Router, and Cisco RV215W Wireless-N VPN Router could allow an unauthenticated, remote attacker to execute arbitrary code on an affected device. The vulnerability is due to improper validation of user-supplied data in the web-based management interface. An attacker could exploit this vulnerability by sending malicious HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system of the affected device as a high-privilege user. RV110W Wireless-N VPN Firewall versions prior to 1.2.2.1 are affected. RV130W Wireless-N Multifunction VPN Router versions prior to 1.0.3.45 are affected. RV215W Wireless-N VPN Router versions prior to 1.3.1.1 are affected.	Fehlende typstrenge Prüfung
20.02.2019	cisco -- hyperflex_hx_data_platform	A vulnerability in the cluster service manager of Cisco HyperFlex Software could allow an unauthenticated, adjacent attacker to execute commands as the root user. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by connecting to the cluster service manager and injecting commands into the bound process. A successful exploit could allow the attacker to run commands on the affected host as the root user. This vulnerability affects Cisco HyperFlex Software releases prior to 3.5(2a).	Fehlende Rechteprüfung

21.02.2019	cisco -- hyperflex_hx_data_platform	A vulnerability in the hxterm service of Cisco HyperFlex Software could allow an unauthenticated, local attacker to gain root access to all nodes in the cluster. The vulnerability is due to insufficient authentication controls. An attacker could exploit this vulnerability by connecting to the hxterm service as a non-privileged, local user. A successful exploit could allow the attacker to gain root access to all member nodes of the HyperFlex cluster. This vulnerability affects Cisco HyperFlex Software Releases prior to 3.5(2a).	Fehlende Rechteprüfung
24.01.2019	cisco -- vsmart_controller	A vulnerability in the vContainer of the Cisco SD-WAN Solution could allow an authenticated, remote attacker to cause a denial of service (DoS) condition and execute arbitrary code as the root user. The vulnerability is due to improper bounds checking by the vContainer. An attacker could exploit this vulnerability by sending a malicious file to an affected vContainer	Fehlende typstrenge Prüfung auf Indexgrenzen

(Fortsetzung)

		instance. A successful exploit could allow the attacker to cause a buffer overflow condition on the affected vContainer, which could result in a DoS condition that the attacker could use to execute arbitrary code as the root user.	
25.01.2016	cisco -- unified_computing_system	An unspecified CGI script in Cisco FX-OS allows remote attackers to execute arbitrary shell commands via a crafted HTTP request, aka Bug ID CSCur90888.	Fehlende typstrenge Prüfung
14.12.2015	cisco -- epc3928_docsis_3.0_8x4_wireless_residential_	Cisco EPC3928 devices allow remote attackers to bypass an intended authentication requirement and execute unspecified administrative functions via a crafted HTTP request, aka Bug ID CSCux24941.	Fehlende typstrenge Prüfung
	gateway_with_embedded_digital_voice_adapter	Cisco EPC3928 devices allow remote attackers to bypass an intended authentication requirement and execute unspecified administrative functions via a crafted HTTP request, aka Bug ID CSCux24941.	Fehlende typstrenge Prüfung

(Fortsetzung)

	cisco -- application_policy_infrastructure_controller	The boot manager in Cisco Application Policy Infrastructure Controller (APIC) 1.1(0.920a) allows local users to bypass intended access restrictions and obtain single-user-mode root access via unspecified vectors, aka Bug ID CSCuu83985.	Fehlende typstrenge Prüfung
	cisco -- prime_network_services_controller	Cisco Prime Network Services Controller 3.0 allows local users to bypass intended access restrictions and execute arbitrary commands via additional parameters to an unspecified command, aka Bug ID CSCus99427.	Fehlende typstrenge Prüfung
	cisco -- application_policy_infrastructure_controller	The boot manager in Cisco Application Policy Infrastructure Controller (APIC) 1.1(0.920a) allows local users to bypass intended access restrictions and obtain single-user-mode root access via unspecified vectors, aka Bug ID CSCuu83985.	Fehlende typstrenge Prüfung
	cisco -- prime_network_services_controller	Cisco Prime Network Services Controller 3.0 allows local users to bypass intended access restrictions and execute arbi-	Fehlende typstrenge Prüfung

(Fortsetzung)

		trary commands via additional parameters to an unspecified command, aka Bug ID CSCus99427.	
30.11.2015	cisco -- ios_xe	Cisco IOS XE 15.4(3)S on ASR 1000 devices improperly loads software packages, which allows local users to bypass license restrictions and obtain certain root privileges by using the CLI to enter crafted filenames, aka Bug ID CSCuv93130.	Fehlende typstrenge Prüfung
02.11.2015	cisco -- web_security_appliance	The admin web interface in Cisco AsyncOS on Web Security Appliance (WSA) devices allows remote authenticated users to obtain root privileges via crafted certificate-generation arguments, aka Bug ID CSCus83445.	Fehlende typstrenge Prüfung
26.10.2015	cisco -- firesight_system_software	The policy implementation in Cisco FireSIGHT Management Center for VMware allows remote authenticated administrators to bypass intended policy restrictions and execute Linux commands as root via unspecified vectors, aka Bug ID CSCuw12839.	Fehlende typstrenge Prüfung

(Fortsetzung)

12.10.2015	cisco -- aironet_access_point_software	Cisco Aironet 1850 access points allow local users to gain privileges via crafted CLI commands, aka Bug ID CSCuv79694.	Fehlende typstrenge Prüfung
05.10.2015	cisco -- vpn_client	Cisco VPN Client uses weak permissions for vpnclient.ini, which allows local users to gain privileges by entering an arbitrary program name in the Command field of the Application Launcher section.	Zugriffsrechte falsch definiert
28.09.2015	cisco -- ios	The SSHv2 functionality in Cisco IOS and IOS XE does not properly implement RSA authentication, which allows remote attackers to obtain login access by leveraging knowledge of a username and the associated public key, aka Bug ID CSCus73013.	Kryptografie falsch implementiert
	cisco -- anyconnect_secure_mobility_client	Cisco AnyConnect Secure Mobility Client on OS X and Linux does not verify pathnames before installation actions, which allows local users to obtain root privileges via a crafted installation file, aka Bug ID CSCuv11947.	Überprüfung von Namen fehlt

(Fortsetzung)

21.09.2015	cisco -- telepresence_server_software	Buffer overflow in the Conference Control Protocol API implementation in Cisco TelePresence Server software, Multiparty Media 310 and 320, and Virtual Machine devices allows remote attackers to cause a denial of service (device crash) via a crafted URL, aka Bug ID CSCuu28277.	Fehlende typstrenge Prüfung

Datum	**Software**	**Text**	**Ursache**
Vmware (virtuelle Maschine) - Auszug (85 Schwachstellen gefunden innerhalb 1 Jahr)			
21.12.2015	vmware -- vcenter_orchestrator	Serialized-object interfaces in VMware vRealize Orchestrator 6.x, vCenter Orchestrator 5.x, vRealize Operations 6.x, vCenter Operations 5.x, and vCenter Application Discovery Manager (vADM) 7.x allow remote attackers to execute arbitrary commands via a crafted serialized Java object, related to the Apache Commons Collections library.	Fehlende typstrenge Prüfung

(Fortsetzung)

26.10.2015	vmware -- vcenter_server	The JMX RMI service in VMware vCenter Server 5.0 before u3e, 5.1 before u3b, 5.5 before u3, and 6.0 before u1 does not restrict registration of MBeans, which allows remote attackers to execute arbitrary code via the RMI protocol.	Überprüfung von Berechtigung fehlt
13.08.2015	vmware -- horizon_view_client	vmware-vmx.exe in VMware Workstation 7.x through 10.x before 10.0.7 and 11.x before 11.1.1, VMware Player 5.x and 6.x before 6.0.7 and 7.x before 7.1.1, and VMware Horizon Client 5.x local-mode before 5.4.2 on Windows does not provide a valid DACL pointer during the setup of the vprintproxy.exe process, which allows host OS users to gain host OS privileges by injecting a thread.	Fehlende typstrenge Prüfung

(Fortsetzung)

Datum	Software	Text	Ursache
Juniper Virtual Private Network (VPN) - Auszug (45 Schwachstellen gefunden innerhalb 1 Jahr)			
21.12.2015	juniper -- screenos	Juniper ScreenOS allows remote attackers to obtain administrative access by entering an unspecified password during a (1) SSH or (2) TELNET session.	Fehlende typstrenge Prüfung
13.07.2015	juniper -- junos	The Juniper SRX Series services gateways with Junos OS do not properly implement the "set system ports console insecure" feature, which allows physically proximate attackers to gain administrative privileges by leveraging access to the console port.	Implementierungsfehler
13.04.2015	juniper -- junos	Juniper Junos allows local users to gain privileges via crafted combinations of CLI commands and arguments.	Fehlende typstrenge Prüfung
13.10.2014	juniper -- srx100	The Juniper SRX Series devices with Junos when an Application Layer Gateway (ALG) is enabled, allows remote attackers to cause a denial of service (flowd crash) via a crafted packet.	Fehlende typstrenge Prüfung
3S Smart Software Solutions CoDeSys (Tool für Automatisierungssysteme) - Auszug (12 Schwachstellen gefunden innerhalb 1 Jahr)			
18.12.2018	3S-Smart Software Solutions GmbH CODESYS Control V3 products	User access management and communication encryption is not enabled by default, which could allow an attacker access to the device and sensitive information, including user credentials.	Fehlende Verschlüsselung

(Fortsetzung)

21.09.2015	3s-smart -- codesys_gateway_server	Multiple heap-based buffer overflows in 3S-Smart CODESYS Gateway Server before 2.3.9.47 allow remote attackers to execute arbitrary code via opcode (1) 0x3ef or (2) 0x3f0.	Fehlende typstrenge Prüfung
21.04.2015	3s-software -- codesys_runtime_system	The Festo CECX-X-C1 Modular Master Controller with CoDeSys and CECX-X-M1 Modular Controller with CoDeSys and SoftMotion provide an undocumented access method involving the FTP protocol, which allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via unspecified vectors.	Fehlerhafte Implementierung
	3s-software -- codesys_runtime_system	The Festo CECX-X-C1 Modular Master Controller with CoDeSys and CECX-X-M1 Modular Controller with CoDeSys and SoftMotion do not require authentication for connections to certain TCP ports, which allows remote attackers to (1) modify the configuration via a request to the debug service on port 4000 or (2) delete log entries via a request to the log service on port 4001.	Fehlerhafte Implementierung
20.05.2013	3s-software -- codesys_gateway-server	Use-after-free vulnerability in the server application in 3S CODESYS Gateway 2.3.9.27 allows remote attackers to cause a denial of service (daemon crash) or possibly execute arbitrary code via unspecified vectors.	Fehlende typstrenge Prüfung

(Fortsetzung)

05.01.2012/ 14.02.2014	3S Smart Software Solutions CoDeSys	Integer Overflow An attacker could exploit this vulnerability by sending specially crafted packets to Port 1217/TCP. Stack Overflow An attacker could exploit this vulnerability by sending an overly long URL to Port 8080/TCP. Content-Length Null Pointer An attacker could exploit this vulnerability by sending a specially crafted Content-Length header to Port 8080/TCP. Invalid HTTP Request Null Pointer An attacker could exploit this vulnerability by sending a request with an unknown HTTP method to Port 8080/TCP. Folders Creation An attacker could exploit this vulnerability by sending a web request containing a nonexistent directory to Port 8080/TCP. Exploitation of this vulnerability results in the creation of arbitrary directories.	Fehlende typstrenge Prüfung

Datum	**Software**	**Text**	**Ursache**
Siemens Simatic - Auszug (60 Schwachstellen gefunden innerhalb 1 Jahr)			
12.02.2019	Siemens SICAM 230	A specially crafted IRP (I/O request packet) can cause the driver to return uninitialized memory, which may result in kernel memory disclosure. A specially crafted IRP (I/O request packet) can cause a buffer overflow resulting in kernel memory corruption,	Buffer Overflow, fehlende typstrenge Prüfung

(Fortsetzung)

		which may allow privilege escalation. A specially crafted TCP packet sent to Port 22347/TCP can cause a heap overflow, which may lead to remote code execution.	
12.02.2019	Siemens EN100 Ethernet Communication Module and SIPROTEC 5 Relays	Specially crafted packets to Port 102/TCP could cause a denial-of-service condition in the affected products. A manual restart is required to recover the EN100 module functionality of the affected devices. Successful exploitation requires an attacker with network access to send multiple packets to the affected products or modules. As a precondition, the IEC 61850-MMS communication needs to be activated on the affected products or modules. No user interaction or privileges are required to exploit the vulnerability. The vulnerability could allow a denial-of-service condition of the network functionality of the device, compromising the availability of the system.	Fehlende typstrenge Prüfung der Eingaben
	Siemens SIMATIC S7-300 CPU	The affected CPUs improperly validate S7 communication packets, which could cause a denial-of-service condition of the CPU. The CPU will remain in DEFECT mode until manual restart.	Fehlende typstrenge Prüfung

(Fortsetzung)

31.08.2015	siemens -- simatic_s7_1200_cpu	Cross-site request forgery (CSRF) vulnerability in the web server on Siemens SIMATIC S7-1200 CPU devices with firmware before 4.1.3 allows remote attackers to hijack the authentication of unspecified victims via unknown vectors.	Fehlende typstrenge Prüfung
20.07.2015	siemens -- siprotec_firmware	The EN100 module with firmware before 4.25 for Siemens SIPROTEC 4 and SIPROTEC Compact devices allows remote attackers to cause a denial of service via crafted packets on UDP port 50000.	Fehlende typstrenge Prüfung
09.03.2015	siemens -- spc4000_firmware	Siemens SPC controllers SPC4000, SPC5000, and SPC6000 before 3.6.0 allow remote attackers to cause a denial of service (device restart) via crafted packets.	Fehlende typstrenge Prüfung

Datum	**Software**	**Text**	**Ursache**
Windturbinensysteme - Auszug (6 Schwachstellen gefunden innerhalb 1 Jahr)			
15.06.2015	rle -- nova-wind_turbine_hmi_firmware	RLE Nova-Wind Turbine HMI devices store cleartext credentials, which allows remote attackers to obtain sensitive information via unspecified vectors.	Fehlende typstrenge Prüfung
01.06.2015	xzeres -- 442sr_os	Cross-site request forgery (CSRF) vulnerability in XZERES 442SR OS on 442SR wind turbines allows remote attackers to hijack the authentication of admins for requests that select a different default admin user via a GET request.	Fehlende typstrenge Prüfung

(Fortsetzung)

30.03.2015	xzeres -- 442sr	Cross-site request forgery (CSRF) vulnerability in XZERES 442SR OS on 442SR wind turbines allows remote attackers to hijack the authentication of admins for requests that modify the default user's password via a GET request.	Fehlerhafte Implementierung
Datum	**Software**	**Text**	**Ursache**
Divers			
27.02.2019	nvidia -- gpu_driver	NVIDIA Windows GPU Display driver contains a vulnerability in the 3D vision component in which the stereo service software, when opening a file, does not check for hard links. This behavior may lead to code execution, denial of service or escalation of privileges.	Fehlerhafte Implementierung
27.02.2019	nvidia -- gpu_driver	NVIDIA Windows GPU Display Driver contains a vulnerability in the kernel mode layer handler for DxgkDdiEscape in which the software uses a sequential operation to read from or write to a buffer, but it uses an incorrect length value that causes it to access memory that is outside of the bounds of the buffer which may lead to denial of service, escalation of privileges, code execution or information disclosure.	Fehlende typstrenge Prüfung - Indexprüfung
28.02.2019	android	In SkSwizzler:onSetSampleX of SkSwizzler.cpp, there is a possible out of bounds write due to a missing bounds check. This could lead to remote escalation of privilege in system_server with no addi-	Fehlende typstrenge Prüfung - Indexprüfung

(Fortsetzung)

		tional execution privileges needed. User interaction is needed for exploitation. Product: Android. Versions: Android-9. Android ID: A-117838472.	

Literatur

[BSI2014] Die Lage der IT-Sicherheit in Deutschland 2014. Bundesamt für Sicherheit in der Informationstechnik – BSI, 53133 Bonn (2014)

[Chip2014] Zeitschrift Chip, 04/2014, S. 38. (2014)

[Euro2014] The Internet Organised Crime Threat Assessment. Europol – European Police Office (2014)

[Kel1988] Keller, H.B.: Echtzeitsimulation zur Prozeßführung komplexer Systeme, Monographie. Fachberichte Simulation. Springer, Berlin (1988)

[Kel1993] Keller, H.B.: Neural nets in environmental applications. In: Avouris, N.M. (Hrsg.): Environmental Informatics: Methodology and Applications of Environmental Informations Processing; Based on the Lectures Given During the Eurocourse on Environmental Informatics Applications, Athinai, GR, June 21–25, 1993, S. 127–146. Kluwer, Dordrecht (1995). (Eurocourses: Computer and Information Science; 6)

[Kel1998] Keller, H.B.: Entwicklung von Software-Systemen mit Ada. Ada-Deutschland Workshop Bremen 1998, FZKA 6177 (1998)

[Kel2004] Keller, H.B.: Ada. In: Henning, P.A. (Hrsg.) Taschenbuch Programmiersprachen, S. 195–214. Fachbuchverlag Leipzig im Carl Hanser, Leipzig (2004)

[Kel2009a] Keller, H.B., Müller, R., Schiedermeier, G., Tempelmeier, T.: Programmierung. In: Benra, J.T. (Hrsg.) Software-Entwicklung für Echtzeitsysteme, S. 129–170. Springer, Berlin (2009)

[Kel2013] Keller, H.B. et al.: Programmiersprachen. Buchbeitrag: Lang, M., Scherber, S.: Perfekte Softwareentwicklung. Symposion, Düsseldorf (2013)

[Kel2015] Keller, H.B.: Technische Informatik. Vorlesungsskript SS 2015. KIT, Fakultät Maschinenbau (2015)

[McC1976] McCabe, T.: A Complexity Measure. IEEE Transactions on Software Engineering, Bd. SE-2, No. 4, December (1976)

[Moo2012] Morre, J.W., et al.: New ISO/IEC Technical Report Describes Vulnerabilities in Programming Languages. CROSSTALK, J. Def. Softw. Eng., March/April 2012, S. 27–30 (2012)

[Ploe2012] Plödereder, E., Dencker, P., Klenk, H., Keller, H.B., Spitzer, S. (Hrsg.): Proceedings Band 210 Automotive – Safety & Security 2012: Sicherheit und Zuverlässigkeit für automobile Informationstechnik Tagung 14.–15.11.2012 in Karlsruhe. Gesellschaft für Informatik e. V., Bonn (2012)

[US2016] Bulletins of the Department of Homeland Security's United States Computer Emergency Readiness Team (US-CERT). https://www.us-cert.gov/ncas/bulletins. Letzter Zugriff am 31.10.2019.

H. B. Keller, *Entwicklung von Echtzeitsystemen*,
https://doi.org/10.1007/978-3-658-26641-7

[VDE2012] VDE-Trendstudie IKT-Sicherheit. VDE Verband der Elektrotechnik Elektronik Informationstechnik e.V., Frankfurt (2012)

[Wai2014] Waibel, P.: Konzeption von Verfahren zur kamerabasierten Analyse und Optimierung von Drehrohrofenprozessen. Schriftenreihe des Instituts für Angewandte Informatik – Automatisierungstechnik, Karlsruher Institut für Technologie; 49. KIT Scientific Publishing, Karlsruhe (2014). isbn:9783731502142

Stichwortverzeichnis

H. B. Keller, *Entwicklung von Echtzeitsystemen*,
https://doi.org/10.1007/978-3-658-26641-7