Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Advisory NCSC-2026-0525

PRIORITEIT: NORMAAL

Kwetsbaarheden verholpen in Linux kernel

Publicatiedatum: 27-11-2026

Toegestane verspreiding: TLP:WHITE
(Traffic Light Protocol)

Deze publicatie bevat het label TLP:WHITE en wordt door het Nationaal Cyber Security Center (NCSC) verspreid. Het NCSC gebruikt het Traffic Light Protocol (TLP) om eenduidig te definiëren wat er met de informatie mag gebeuren. Wanneer informatie is voorzien van een TLP-aanduiding weet u met wie u deze informatie mag de-len. Dit staat beschreven in de standaard First (www.first.org/tlp).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Reacties zijn welkom op info@ncsc.nl.

Feiten

De Linux kernel ontwikkelaars hebben meerdere kwetsbaarheden verholpen in diverse subsystemen en drivers, waaronder IPv6, KVM, SUNRPC, NFS, SMB, XFS, overlayfs, OCFS2, media drivers, netwerkdrivers, geheugenbeheer, en meer.

Duiding

De kwetsbaarheden betreffen onder andere use-after-free, race conditions, out-of-bounds reads/writes, null pointer dereferences, deadlocks, en improper synchronisatie. Aanvallers kunnen deze kwetsbaarheden lokaal of, in enkele gevallen, via netwerktoegang misbruiken om denial of service te veroorzaken, kernel crashes te triggeren, geheugen corruptie te bewerkstelligen, of in beperkte gevallen privileges te escaleren. Sommige kwetsbaarheden zijn specifiek voor bepaalde hardware of configuraties, zoals Intel TDX, AMD GPU's, of specifieke netwerkprotocollen. De patches corrigeren onder andere foutieve geheugenreferenties, verbeteren synchronisatie en locking, valideren invoerparameters, en zorgen voor correcte resource- en foutafhandeling binnen de kernelcomponenten.

Een zeer ernstige kwetsbaarheid die is verholpen heeft kenmerk CVE-2026-99362 toegewezen gekregen en stelt een kwaadwillende in staat om zonder voorafgaande authenticatie willekeurige code uit te voeren op het kwetsbare systeem. Onderzoekers hebben Proof-of-Concept-code en een write-up gepubliceerd waarin ze aantonen een remote rootshell te kunnen installeren en gebruiken. Voor succesvol misbruik moet de kwaadwillende toegang hebben tot de nfs poort, TCP/2049. Het is ongebruikelijk dat deze poort publiek toegankelijk is buiten de eigen infrastructuur.

Oplossingen

Linux kernel ontwikkelaars hebben updates uitgebracht die de beschreven kwetsbaarheden verhelpen door codewijzigingen in de betreffende subsystemen en drivers. Gebruikers wordt geadviseerd om de meest recente kernelversies te installeren waarin deze fixes zijn opgenomen. Zie bijgevoegde referenties voor meer informatie.

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-99678	7.1 HIGH
CVE-2026-99679	7.2 HIGH
CVE-2026-99680	2.3 LOW
CVE-2026-99681	4.1 MEDIUM
CVE-2026-99682	
CVE-2026-99683	6.7 MEDIUM
CVE-2026-99684	4.1 MEDIUM
CVE-2026-99685	8.4 HIGH
CVE-2026-99686	2.1 LOW
CVE-2026-99687	5.1 MEDIUM
CVE-2026-99688	7.3 HIGH
CVE-2026-99689	5.3 MEDIUM
CVE-2026-99690	7.3 HIGH
CVE-2026-99691	7.1 HIGH
CVE-2026-99692	5.5 MEDIUM
CVE-2026-99693	6.2 MEDIUM
CVE-2026-99694	4.8 MEDIUM
CVE-2026-99695	6.9 MEDIUM
CVE-2026-99696	6.9 MEDIUM
CVE-2026-99320	8.5 HIGH
CVE-2026-99332	2.4 LOW
CVE-2026-99335	5.6 MEDIUM
CVE-2026-99336	7.0 HIGH
CVE-2026-99337	8.2 HIGH
CVE-2026-99338	5.1 MEDIUM
CVE-2026-99339	5.1 MEDIUM
CVE-2026-99340	7.8 HIGH
CVE-2026-99341	1.8 LOW

CVE	CVSS Score
CVE-2026-99353	4.4 MEDIUM
CVE-2026-99354	4.1 MEDIUM
CVE-2026-99355	9.2 CRITICAL
CVE-2026-99356	8.8 HIGH
CVE-2026-99357	7.6 HIGH
CVE-2026-99358	6.9 MEDIUM
CVE-2026-99359	
CVE-2026-99360	4.1 MEDIUM
CVE-2026-99361	8.2 HIGH
CVE-2026-99362	9.3 CRITICAL
CVE-2026-99363	6.3 MEDIUM
CVE-2026-99364	5.7 MEDIUM
CVE-2026-99365	6.8 MEDIUM
CVE-2026-99366	9.2 CRITICAL
CVE-2026-99367	4.4 MEDIUM
CVE-2026-99368	2.3 LOW
CVE-2026-99369	8.7 HIGH
CVE-2026-99370	5.3 MEDIUM
CVE-2026-99371	6.9 MEDIUM
CVE-2026-99372	6.7 MEDIUM
CVE-2026-99373	4.8 MEDIUM
CVE-2026-99374	6.0 MEDIUM
CVE-2026-99375	5.8 MEDIUM
CVE-2026-99376	5.7 MEDIUM
CVE-2026-99377	7.1 HIGH
CVE-2026-99378	4.1 MEDIUM
CVE-2026-99379	6.0 MEDIUM
CVE-2026-99380	7.1 HIGH
CVE-2026-99381	2.3 LOW
CVE-2026-99382	5.3 MEDIUM
CVE-2026-99383	7.1 HIGH

CVE	CVSS Score
CVE-2026-99384	7.1 HIGH
CVE-2026-99385	9.8 CRITICAL
CVE-2026-99386	7.3 HIGH
CVE-2026-99387	7.1 HIGH
CVE-2026-99388	8.7 HIGH
CVE-2026-99389	7.7 HIGH
CVE-2026-99390	
CVE-2026-99391	
CVE-2026-99392	
CVE-2026-99393	
CVE-2026-99394	
CVE-2026-99395	7.2 HIGH
CVE-2026-99396	7.1 HIGH
CVE-2026-99397	
CVE-2026-99398	
CVE-2026-99399	6.1 MEDIUM
CVE-2026-99400	7.2 HIGH
CVE-2026-99401	7.0 HIGH
CVE-2026-99402	
CVE-2026-99403	4.4 MEDIUM
CVE-2026-99404	5.5 MEDIUM
CVE-2026-99405	
CVE-2026-99406	
CVE-2026-99407	
CVE-2026-99408	
CVE-2026-99409	
CVE-2026-99410	
CVE-2026-99411	
CVE-2026-99412	
CVE-2026-99413	4.4 MEDIUM
CVE-2026-99414	6.8 MEDIUM

CVE	CVSS Score
CVE-2026-99415	4.8 MEDIUM
CVE-2026-99416	6.9 MEDIUM
CVE-2026-99417	5.8 MEDIUM
CVE-2026-99418	6.8 MEDIUM
CVE-2026-99419	5.8 MEDIUM
CVE-2026-99420	5.7 MEDIUM
CVE-2026-99421	
CVE-2026-99422	7.3 HIGH
CVE-2026-99423	7.3 HIGH
CVE-2026-99424	7.3 HIGH
CVE-2026-99425	7.3 HIGH
CVE-2026-99426	4.1 MEDIUM
CVE-2026-99427	6.0 MEDIUM
CVE-2026-99428	5.7 MEDIUM
CVE-2026-99429	7.3 HIGH
CVE-2026-99430	7.1 HIGH
CVE-2026-99431	4.1 MEDIUM
CVE-2026-99432	7.7 HIGH
CVE-2026-99433	8.8 HIGH
CVE-2026-99434	4.1 MEDIUM
CVE-2026-99435	7.1 HIGH
CVE-2026-99436	5.4 MEDIUM
CVE-2026-99437	5.4 MEDIUM
CVE-2026-99438	5.7 MEDIUM
CVE-2026-99439	5.4 MEDIUM
CVE-2026-99440	4.1 MEDIUM
CVE-2026-99441	9.2 CRITICAL
CVE-2026-99442	5.7 MEDIUM
CVE-2026-99443	4.4 MEDIUM
CVE-2026-99444	4.1 MEDIUM
CVE-2026-99445	4.1 MEDIUM

CVE	CVSS Score
CVE-2026-99446	4.1 MEDIUM
CVE-2026-99447	4.1 MEDIUM
CVE-2026-99448	7.1 HIGH
CVE-2026-99449	4.1 MEDIUM
CVE-2026-99450	4.1 MEDIUM
CVE-2026-99451	7.7 HIGH
CVE-2026-99452	4.1 MEDIUM
CVE-2026-99453	4.1 MEDIUM
CVE-2026-99454	7.7 HIGH
CVE-2026-99455	4.4 MEDIUM
CVE-2026-99456	4.1 MEDIUM
CVE-2026-99457	7.3 HIGH
CVE-2026-99458	4.4 MEDIUM
CVE-2026-99459	5.5 MEDIUM
CVE-2026-99460	9.2 CRITICAL
CVE-2026-99461	4.7 MEDIUM
CVE-2026-99462	7.3 HIGH
CVE-2026-99463	7.3 HIGH
CVE-2026-99464	5.2 MEDIUM
CVE-2026-99465	6.7 MEDIUM
CVE-2026-99466	4.1 MEDIUM
CVE-2026-99467	4.7 MEDIUM
CVE-2026-99468	7.3 HIGH
CVE-2026-99469	5.4 MEDIUM
CVE-2026-99470	4.4 MEDIUM
CVE-2026-99471	7.1 HIGH
CVE-2026-99472	7.1 HIGH
CVE-2026-99473	7.3 HIGH
CVE-2026-99474	4.7 MEDIUM
CVE-2026-99475	4.1 MEDIUM
CVE-2026-99476	7.0 HIGH

CVE	CVSS Score
CVE-2026-99477	7.3 HIGH
CVE-2026-99478	7.3 HIGH
CVE-2026-99479	4.1 MEDIUM
CVE-2026-99480	7.3 HIGH
CVE-2026-99481	4.4 MEDIUM
CVE-2026-99482	4.1 MEDIUM
CVE-2026-99483	6.9 MEDIUM
CVE-2026-99484	7.3 HIGH
CVE-2026-99485	7.3 HIGH
CVE-2026-99486	6.1 MEDIUM
CVE-2026-99487	5.5 MEDIUM
CVE-2026-99488	4.1 MEDIUM
CVE-2026-99489	7.0 HIGH
CVE-2026-99490	5.4 MEDIUM
CVE-2026-99491	5.4 MEDIUM
CVE-2026-99492	4.1 MEDIUM
CVE-2026-99493	4.7 MEDIUM
CVE-2026-99494	6.1 MEDIUM
CVE-2026-99495	6.3 MEDIUM
CVE-2026-99496	3.4 LOW
CVE-2026-99497	7.8 HIGH
CVE-2026-99498	4.4 MEDIUM
CVE-2026-99499	4.1 MEDIUM
CVE-2026-99500	
CVE-2026-99501	4.4 MEDIUM
CVE-2026-99502	4.1 MEDIUM
CVE-2026-99503	4.1 MEDIUM
CVE-2026-99504	4.4 MEDIUM
CVE-2026-99505	4.4 MEDIUM
CVE-2026-99506	7.3 HIGH
CVE-2026-99507	7.3 HIGH

CVE	CVSS Score
CVE-2026-99508	4.1 MEDIUM
CVE-2026-99509	5.5 MEDIUM
CVE-2026-99510	7.3 HIGH
CVE-2026-99511	4.1 MEDIUM
CVE-2026-99512	5.4 MEDIUM
CVE-2026-99513	9.8 CRITICAL
CVE-2026-99514	2.0 LOW
CVE-2026-99515	7.3 HIGH
CVE-2026-99516	6.0 MEDIUM
CVE-2026-99517	6.9 MEDIUM
CVE-2026-99518	4.4 MEDIUM
CVE-2026-99519	
CVE-2026-99520	4.4 MEDIUM
CVE-2026-99521	5.5 MEDIUM
CVE-2026-99522	8.4 HIGH
CVE-2026-99523	7.3 HIGH
CVE-2026-99524	4.1 MEDIUM
CVE-2026-99525	4.7 MEDIUM
CVE-2026-99526	7.1 HIGH
CVE-2026-99527	4.4 MEDIUM
CVE-2026-99528	7.3 HIGH
CVE-2026-99529	4.4 MEDIUM
CVE-2026-99530	7.3 HIGH
CVE-2026-99531	7.7 HIGH
CVE-2026-99532	8.7 HIGH
CVE-2026-99533	7.1 HIGH
CVE-2026-99534	5.3 MEDIUM
CVE-2026-99535	7.2 HIGH
CVE-2026-99536	8.6 HIGH
CVE-2026-99537	5.3 MEDIUM
CVE-2026-99538	6.8 MEDIUM

CVE	CVSS Score
CVE-2026-99539	7.1 HIGH
CVE-2026-99540	9.2 CRITICAL
CVE-2026-99541	7.2 HIGH
CVE-2026-99542	7.1 HIGH
CVE-2026-99543	4.4 MEDIUM
CVE-2026-99544	8.6 HIGH
CVE-2026-99545	4.1 MEDIUM
CVE-2026-99546	7.3 HIGH
CVE-2026-99547	4.1 MEDIUM
CVE-2026-99548	5.7 MEDIUM
CVE-2026-99549	7.1 HIGH
CVE-2026-99550	4.4 MEDIUM
CVE-2026-99551	4.1 MEDIUM
CVE-2026-99552	4.1 MEDIUM
CVE-2026-99553	4.7 MEDIUM
CVE-2026-99554	7.0 HIGH
CVE-2026-99555	5.7 MEDIUM
CVE-2026-99556	7.7 HIGH
CVE-2026-99557	6.0 MEDIUM
CVE-2026-99558	4.4 MEDIUM
CVE-2026-99559	6.8 MEDIUM
CVE-2026-99560	4.4 MEDIUM
CVE-2026-99561	5.7 MEDIUM
CVE-2026-99562	6.0 MEDIUM
CVE-2026-99563	8.7 HIGH
CVE-2026-99564	8.7 HIGH
CVE-2026-99565	8.3 HIGH
CVE-2026-99594	2.3 LOW
CVE-2026-99596	
CVE-2026-99597	4.1 MEDIUM
CVE-2026-99598	5.7 MEDIUM

CVE	CVSS Score
CVE-2026-99599	7.1 HIGH
CVE-2026-99600	4.8 MEDIUM
CVE-2026-99601	7.2 HIGH
CVE-2026-99602	7.1 HIGH
CVE-2026-99603	7.8 HIGH
CVE-2026-99605	
CVE-2026-99606	5.5 MEDIUM
CVE-2026-99607	9.8 CRITICAL
CVE-2026-99608	5.7 MEDIUM
CVE-2026-99609	7.8 HIGH
CVE-2026-99610	2.4 LOW
CVE-2026-99611	7.8 HIGH
CVE-2026-99612	4.7 MEDIUM
CVE-2026-99613	5.5 MEDIUM
CVE-2026-99614	5.5 MEDIUM
CVE-2026-99615	
CVE-2026-99616	5.5 MEDIUM
CVE-2026-99617	4.4 MEDIUM
CVE-2026-99618	7.5 HIGH
CVE-2026-99619	4.7 MEDIUM
CVE-2026-99620	4.7 MEDIUM
CVE-2026-99621	5.5 MEDIUM
CVE-2026-99622	
CVE-2026-99623	4.4 MEDIUM
CVE-2026-99624	4.7 MEDIUM
CVE-2026-99625	7.0 HIGH
CVE-2026-99626	
CVE-2026-99627	7.1 HIGH
CVE-2026-99628	5.5 MEDIUM
CVE-2026-99629	5.5 MEDIUM
CVE-2026-99630	7.0 HIGH

CVE	CVSS Score
CVE-2026-99631	5.5 MEDIUM
CVE-2026-99632	5.5 MEDIUM
CVE-2026-99633	5.5 MEDIUM
CVE-2026-99634	9.8 CRITICAL
CVE-2026-99635	6.0 MEDIUM
CVE-2026-99636	7.5 HIGH
CVE-2026-99637	5.5 MEDIUM
CVE-2026-99638	5.5 MEDIUM
CVE-2026-99639	3.3 LOW
CVE-2026-99640	
CVE-2026-99641	
CVE-2026-99642	
CVE-2026-99643	5.7 MEDIUM
CVE-2026-99644	5.5 MEDIUM
CVE-2026-99645	7.0 HIGH
CVE-2026-99646	5.7 MEDIUM
CVE-2026-99647	
CVE-2026-99648	7.0 HIGH
CVE-2026-99649	5.7 MEDIUM
CVE-2026-99650	2.0 LOW
CVE-2026-99651	6.4 MEDIUM
CVE-2026-99652	5.7 MEDIUM
CVE-2026-99653	5.7 MEDIUM
CVE-2026-99654	2.0 LOW
CVE-2026-99655	6.5 MEDIUM
CVE-2026-99656	2.0 LOW
CVE-2026-99657	7.3 HIGH
CVE-2026-99658	5.7 MEDIUM
CVE-2026-99659	7.3 HIGH
CVE-2026-99660	5.7 MEDIUM
CVE-2026-99661	7.3 HIGH

CVE	CVSS Score
CVE-2026-99662	6.7 MEDIUM
CVE-2026-99663	
CVE-2026-99664	
CVE-2026-99665	4.8 MEDIUM
CVE-2026-99666	5.7 MEDIUM
CVE-2026-99667	7.3 HIGH
CVE-2026-99668	7.1 HIGH
CVE-2026-99669	5.7 MEDIUM
CVE-2026-99670	6.8 MEDIUM
CVE-2026-99671	6.8 MEDIUM
CVE-2026-99672	7.3 HIGH
CVE-2026-99673	6.8 MEDIUM
CVE-2026-99674	6.8 MEDIUM
CVE-2026-99675	8.7 HIGH
CVE-2026-99676	9.2 CRITICAL
CVE-2026-99677	7.2 HIGH
CVE-2026-99697	7.3 HIGH
CVE-2026-99698	5.5 MEDIUM
CVE-2026-99699	5.7 MEDIUM
CVE-2026-99700	5.7 MEDIUM
CVE-2026-99701	2.0 LOW
CVE-2026-99702	2.0 LOW
CVE-2026-99703	6.8 MEDIUM
CVE-2026-99704	4.8 MEDIUM
CVE-2026-99705	5.7 MEDIUM
CVE-2026-99706	7.3 HIGH
CVE-2026-99707	7.3 HIGH
CVE-2026-99708	6.8 MEDIUM
CVE-2026-99709	8.5 HIGH
CVE-2026-99710	8.2 HIGH
CVE-2026-99711	6.9 MEDIUM

CVE	CVSS Score
CVE-2026-99712	6.9 MEDIUM
CVE-2026-99713	6.9 MEDIUM
CVE-2026-99714	4.1 MEDIUM
CVE-2026-99715	7.5 HIGH
CVE-2026-99716	4.1 MEDIUM
CVE-2026-99717	5.5 MEDIUM
CVE-2026-99718	4.1 MEDIUM
CVE-2026-99719	4.8 MEDIUM
CVE-2026-99720	4.1 MEDIUM
CVE-2026-99721	5.2 MEDIUM
CVE-2026-99722	8.2 HIGH
CVE-2026-99723	3.3 LOW
CVE-2026-99724	7.3 HIGH
CVE-2026-99725	8.5 HIGH
CVE-2026-99726	2.0 LOW
CVE-2026-99727	7.0 HIGH
CVE-2026-99728	7.3 HIGH
CVE-2026-99729	5.8 MEDIUM
CVE-2026-99730	7.3 HIGH
CVE-2026-99731	5.7 MEDIUM
CVE-2026-99732	4.7 MEDIUM
CVE-2026-99733	2.0 LOW
CVE-2026-99734	5.8 MEDIUM
CVE-2026-99735	7.3 HIGH
CVE-2026-99736	5.5 MEDIUM
CVE-2026-99737	5.7 MEDIUM
CVE-2026-99738	5.7 MEDIUM
CVE-2026-99739	5.7 MEDIUM
CVE-2026-99740	5.7 MEDIUM
CVE-2026-99741	3.3 LOW
CVE-2026-99742	6.8 MEDIUM

CVE	CVSS Score
CVE-2026-99743	6.3 MEDIUM
CVE-2026-99744	7.1 HIGH
CVE-2026-99745	5.7 MEDIUM
CVE-2026-99746	7.0 HIGH
CVE-2026-99747	5.5 MEDIUM
CVE-2026-99748	2.3 LOW
CVE-2026-99749	5.3 MEDIUM
CVE-2026-99750	2.3 LOW
CVE-2026-99751	6.7 MEDIUM
CVE-2026-99752	5.7 MEDIUM
CVE-2026-99753	7.3 HIGH
CVE-2026-99754	8.8 HIGH
CVE-2026-99755	7.3 HIGH
CVE-2026-99756	5.8 MEDIUM
CVE-2026-99757	5.5 MEDIUM
CVE-2026-99758	8.7 HIGH
CVE-2026-99759	2.0 LOW
CVE-2026-99760	7.1 HIGH
CVE-2026-99761	7.3 HIGH
CVE-2026-99762	7.7 HIGH
CVE-2026-99763	5.5 MEDIUM
CVE-2026-99764	6.5 MEDIUM
CVE-2026-99765	5.9 MEDIUM
CVE-2026-99766	4.4 MEDIUM
CVE-2026-99767	8.3 HIGH
CVE-2026-99768	2.0 LOW
CVE-2026-99769	6.8 MEDIUM
CVE-2026-99770	5.7 MEDIUM
CVE-2026-99771	2.3 LOW
CVE-2026-99772	5.7 MEDIUM
CVE-2026-99773	7.3 HIGH

CVE	CVSS Score
CVE-2026-99774	5.7 MEDIUM
CVE-2026-99775	7.3 HIGH
CVE-2026-99776	4.1 MEDIUM
CVE-2026-99777	4.4 MEDIUM
CVE-2026-99778	3.3 LOW
CVE-2026-99779	5.1 MEDIUM
CVE-2026-99780	4.4 MEDIUM
CVE-2026-99781	5.1 MEDIUM
CVE-2026-99782	
CVE-2026-99783	4.4 MEDIUM
CVE-2026-99784	7.1 HIGH
CVE-2026-99785	8.4 HIGH
CVE-2026-99786	4.8 MEDIUM
CVE-2026-99787	4.7 MEDIUM
CVE-2026-99788	4.4 MEDIUM
CVE-2026-99789	6.9 MEDIUM
CVE-2026-99790	5.6 MEDIUM
CVE-2026-99791	5.5 MEDIUM
CVE-2026-99792	7.7 HIGH
CVE-2026-99793	2.3 LOW
CVE-2026-99794	8.7 HIGH
CVE-2026-99795	4.4 MEDIUM
CVE-2026-99796	6.8 MEDIUM
CVE-2026-99797	6.8 MEDIUM
CVE-2026-99798	7.3 HIGH
CVE-2026-99799	6.8 MEDIUM
CVE-2026-99800	7.3 HIGH
CVE-2026-99801	7.1 HIGH
CVE-2026-99802	4.8 MEDIUM
CVE-2026-99803	4.8 MEDIUM
CVE-2026-99804	7.3 HIGH

CWE's

CWE	Beschrijving
CWE-22	Improper Limitation of a Pathname to a Restricted Directory
CWE-115	Misinterpretation of Input
CWE-120	Buffer Copy without Checking Size of Input
CWE-121	Stack-based Buffer Overflow
CWE-125	Out-of-bounds Read
CWE-130	Improper Handling of Length Parameter Inconsistency
CWE-178	Improper Handling of Case Sensitivity
CWE-179	Incorrect Behavior Order: Early Validation
CWE-190	Integer Overflow or Wraparound
CWE-191	Integer Underflow (Wrap or Wraparound)
CWE-253	Incorrect Check of Function Return Value
CWE-266	Incorrect Privilege Assignment
CWE-270	Privilege Context Switching Error
CWE-281	Improper Preservation of Permissions
CWE-283	Unverified Ownership
CWE-305	Authentication Bypass by Primary Weakness
CWE-358	Improperly Implemented Security Check for Standard
CWE-362	Concurrent Execution using Shared Resource with Improper Synchronization
CWE-366	Race Condition within a Thread
CWE-367	Time-of-check Time-of-use (TOCTOU) Race Condition
CWE-369	Divide By Zero
CWE-385	Covert Timing Channel
CWE-392	Missing Report of Error Condition
CWE-401	Missing Release of Memory after Effective Lifetime
CWE-404	Improper Resource Shutdown or Release
CWE-412	Unrestricted Externally Accessible Lock
CWE-413	Improper Resource Locking
CWE-415	Double Free
CWE-416	Use After Free

CWE	Beschrijving
CWE-459	Incomplete Cleanup
CWE-476	NULL Pointer Dereference
CWE-606	Unchecked Input for Loop Condition
CWE-617	Reachable Assertion
CWE-653	Improper Isolation or Compartmentalization
CWE-667	Improper Locking
CWE-681	Incorrect Conversion between Numeric Types
CWE-749	Exposed Dangerous Method or Function
CWE-770	Allocation of Resources Without Limits or Throttling
CWE-771	Missing Reference to Active Allocated Resource
CWE-772	Missing Release of Resource after Effective Lifetime
CWE-787	Out-of-bounds Write
CWE-805	Buffer Access with Incorrect Length Value
CWE-820	Missing Synchronization
CWE-821	Incorrect Synchronization
CWE-823	Use of Out-of-range Pointer Offset
CWE-825	Expired Pointer Dereference
CWE-826	Premature Release of Resource During Expected Lifetime
CWE-833	Deadlock
CWE-835	Loop with Unreachable Exit Condition
CWE-841	Improper Enforcement of Behavioral Workflow
CWE-843	Access of Resource Using Incompatible Type
CWE-908	Use of Uninitialized Resource
CWE-909	Missing Initialization of Resource
CWE-911	Improper Update of Reference Count
CWE-1050	Excessive Platform Resource Consumption within a Loop
CWE-1285	Improper Validation of Specified Index, Position, or Offset in Input
CWE-1288	Improper Validation of Consistency within Input
CWE-1335	Incorrect Bitwise Shift of Integer
CWE-1341	Multiple Releases of Same Resource or Handle

Getroffen producten

Debian
Debian Linux

Linux
Kernel

NetApp
Linux kernel

Oracle
Oracle Linux

RESF
RESF Rocky Linux

Red Hat
Red Hat Enterprise Linux
kernel

Ubuntu
linux

Disclaimer

The Netherlands Cyber Security Center (henceforth: NCSC-NL) maintains this page to enhance access to its information and security advisories. The use of this security advisory is subject to the following terms and conditions:
NCSC-NL makes every reasonable effort to ensure that the content of this page is kept up to date, and that it is accurate and complete. Nevertheless, NCSC-NL cannot entirely rule out the possibility of errors, and therefore cannot give any warranty in respect of its completeness, accuracy or continuous keeping up-to-date. The information contained in this security advisory is intended solely for the purpose of providing general information to professional users. No rights can be derived from the information provided therein. NCSC-NL and the Kingdom of the Netherlands assume no legal liability or responsibility for any damage resulting from either the use or inability of use of this security advisory. This includes damage resulting from the inaccuracy of incompleteness of the information contained in the advisory. This security advisory is subject to Dutch law. All disputes related to or arising from the use of this advisory will be submitted to the competent court in The Hague. This choice of means also applies to the court in summary proceedings.