Software@LTH, March 4, 2020

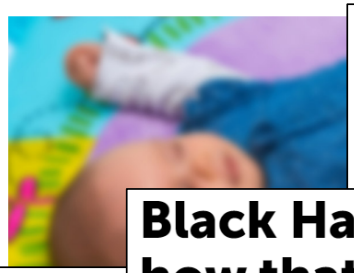
Vulnerabilities in third party code - when someone else's problems become yours

Martin Hell

1. Dept. of Electrical and Information Technology
Lund University, Sweden

2. Debricked AB (Spinoff from Vinnova SECONDS project)

Hacker terrorizes family by hijacking baby monitor



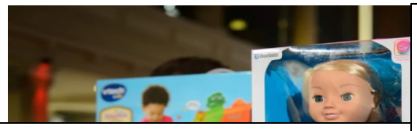
'Internet of things' or 'vulnerability of everything'? Japan will hack its own citizens to find out

By James Griffiths, CNN

Updated 0259 GMT (1059 HKT) February 2, 2019

News & buzz

This pretty blond doll could be spying on your family



Hackers once stole a casino's high-roller database through a thermometer in the lobby fish tank

Oscar Williams-Grut Apr 15, 2018, 9:08 AM

Black Hat USA 2015: The … how that Jeep was hacke…

Recently we wrote about the Jeep Cherokee hack incident. At B… Charlie Miller and Chris Valasek finally explained, how exactly th… happened.

Alex Drozhzhin

A new 'sr… your wifi…

Ethan Chiel
10/15/15 3:36PM • Fil…

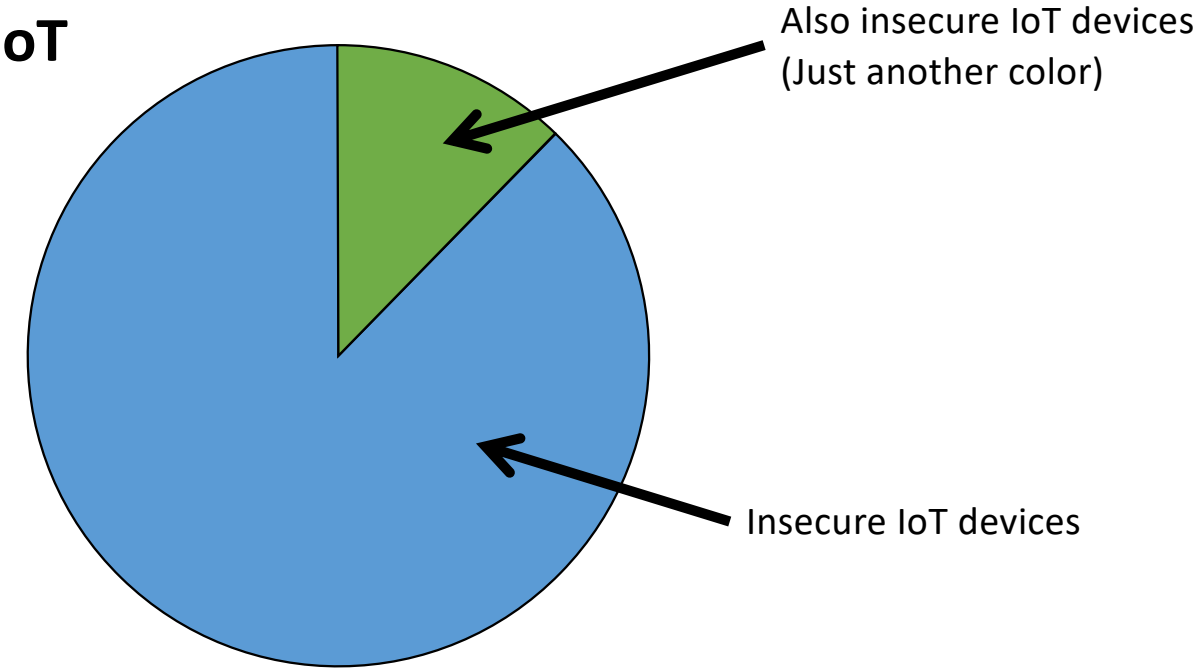
DDoS attack that disrupted internet was largest of its kind in history, experts say

Dyn, the victim of last week's denial of service attack, said it was orchestrated using a weapon called the Mirai botnet as the 'primary source of malicious attack'

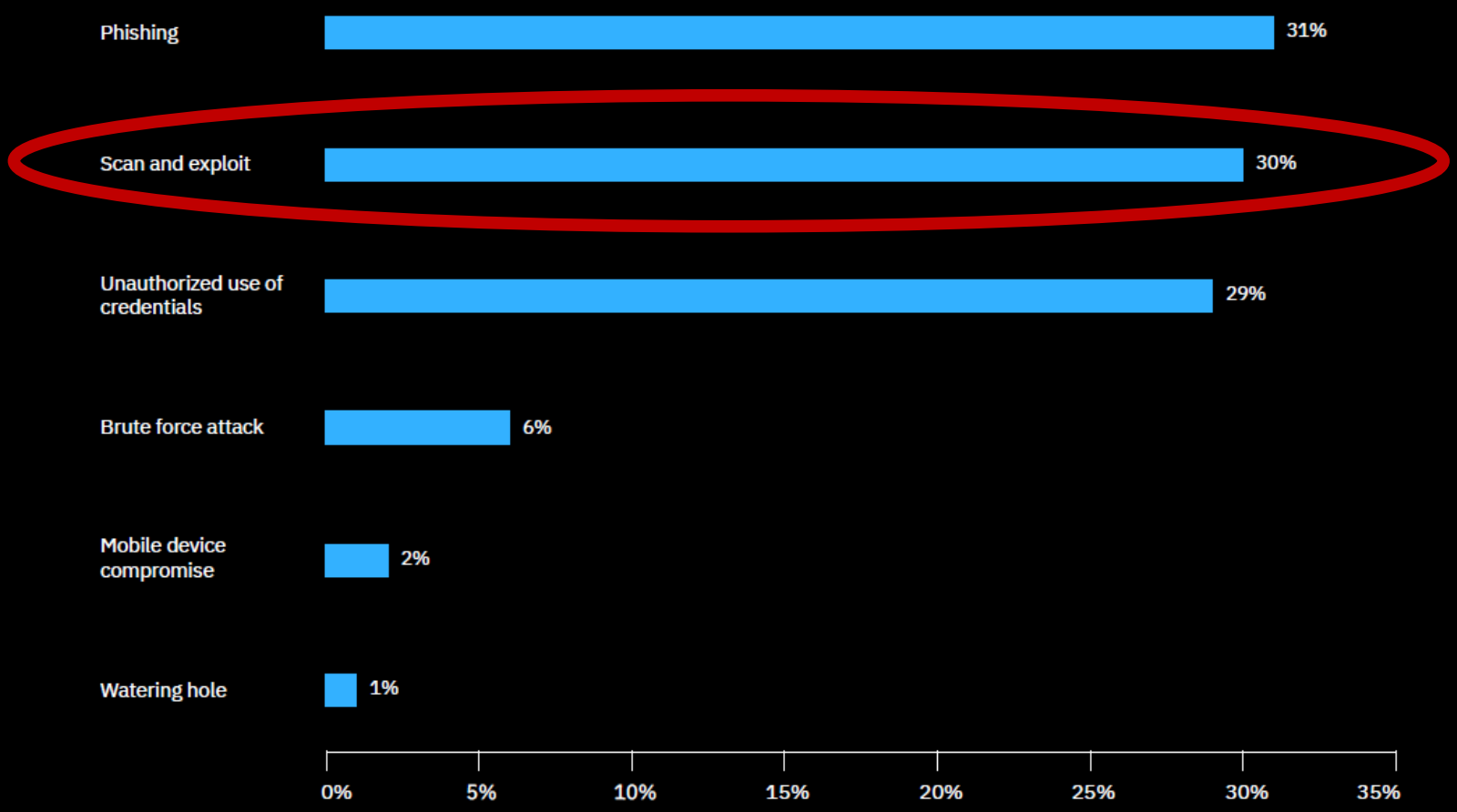
- **Major cyber attack disrupts internet service across Europe and US**

IoT Security

Security is a huge problem in IoT

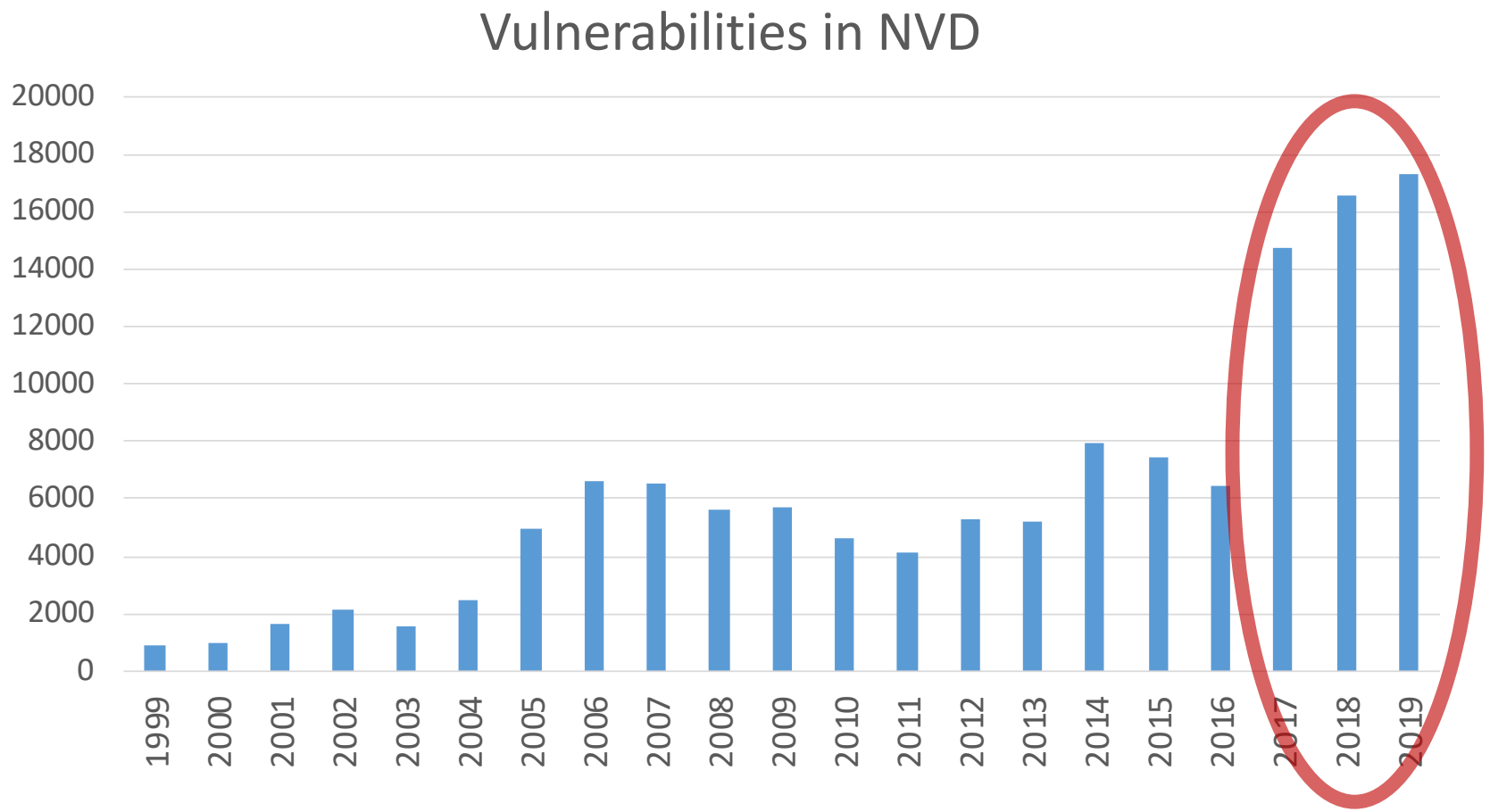


Top Access Vectors 2019

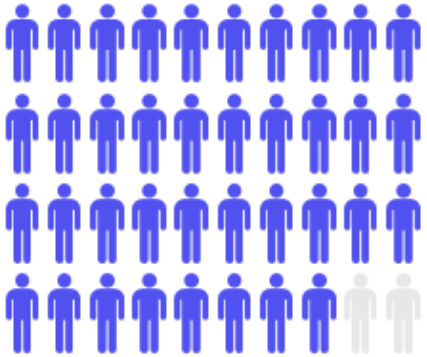


Source: IBM - X-Force Threat Intelligence Index 2020

Number of Vulnerabilities



Usage of Open Source

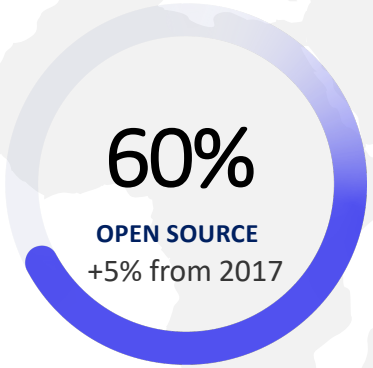


96%

OF ALL COMPANIES

96% of all companies use any Open Source in their software development.

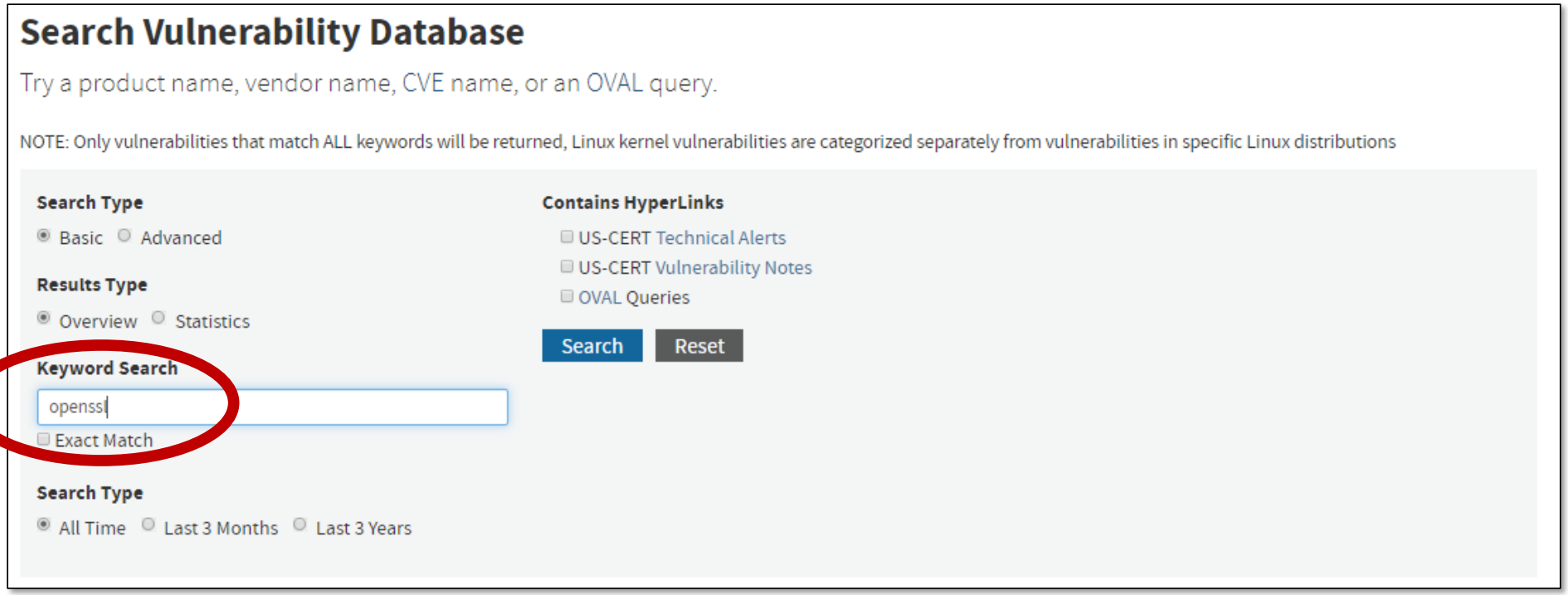
- Synopsys 2019



More than half of the codebase is based on open source in companies using open source.

-Synopsys 2019

Find your vulnerabilities



https://nvd.nist.gov

Problems and Debricked's approach

Manual effort
Problem: Time consuming and error prone
Solution: Match automatically and keep database constantly updated

Transitive dependencies
Problem: Some dependencies require their own dependencies
Solution: Automatically find all transitive dependencies

Other security issues
Problem: Not everything is found in NVD, 8% of GitHub issues are security related
Solution: Scrape and classify GitHub issues (and other sources) using NLP

Time delay
Problem: It can take days or weeks before NVD lists all vulnerable software
Solution: Analyzes the vulnerability text with NER and extract vulnerable versions

Generic severity scoring
Problem: The severity scoring is not tailored to environment/system/device
Solution: Built a recommender system that learns user preferences

Tracking analyzed vulnerabilities
Problem: You need to remember which vulnerabilities are not applicable and which need a fix
Solution: Allow removal of vulnerabilities that are of no interest and automatically fix vulnerabilities of interest

debricked

- Repositories
- Vulnerabilities
- Dependencies
- Manage
- Admin tools

benchmark debricked

Vulnerabilities | All commits | Dependencies

15 entries

Name	Published	CVSS3	CVSS2	debAI	Dependencies	Review status	Fixes and exploits	Ticket status
CVE-2019-11835	2019-05-09	9.8	7.5	59	cjson_proj...	Unexamined	3 1	0 0 0
CVE-2019-11834	2019-05-09	9.8	7.5	59	cjson_proj...	Unexamined	3 1	0 0 0
CVE-2018-11218	2018-06-17	9.8	7.5	59	redislabs r...	Unaffected	11 2	0 0 0
CVE-2019-10744	2019-07-26	9.8	7.5	59	lodash	Unexamined		0 0 0
CVE-2019-5413	2019-03-21	9.8	7.5	59	morgan_pr...	Unexamined	1 1	0 0 0
CVE-2018-16492	2019-02-01	9.8	7.5	59	extend_pr...	Unexamined		0 0 0
CVE-2019-15599	2019-12-18	9.8	7.5	41	tree-kill_pr...	Unexamined		0 0 0
CVE-2018-16487	2019-02-01	9.8	7.5	59	lodash	Unexamined		0 0 0
CVE-2018-11219	2018-06-17	9.8	7.5	59	redislabs r...	Unexamined	11 1	0 0 0
CVE-2019-10746	2019-08-23	9.8	7.5	41	mixin-dee...	Unexamined		0 0 0
CVE-2018-10002...	2018-08-20	9.8	7.5	59	cjson_proj...	Vulnerable		0 0 0
CVE-2018-10006...	2018-07-09	9.8	5	50	cryptiles_p...	Unaffected		0 0 0

Research Projects

Smarty (SSF)

- Smart City
- Deploying updates
- Vulnerability analysis
- Device management

HATCH (Vinnova)

- Handling Vulnerabilities in the Value Chain
- Views for integrators
- Communication of vulnerabilities

SecT (Vinnova)

- Interaction design within security
- Meeting needs of different roles
- Cloud deployment and onboarding

Example from Research

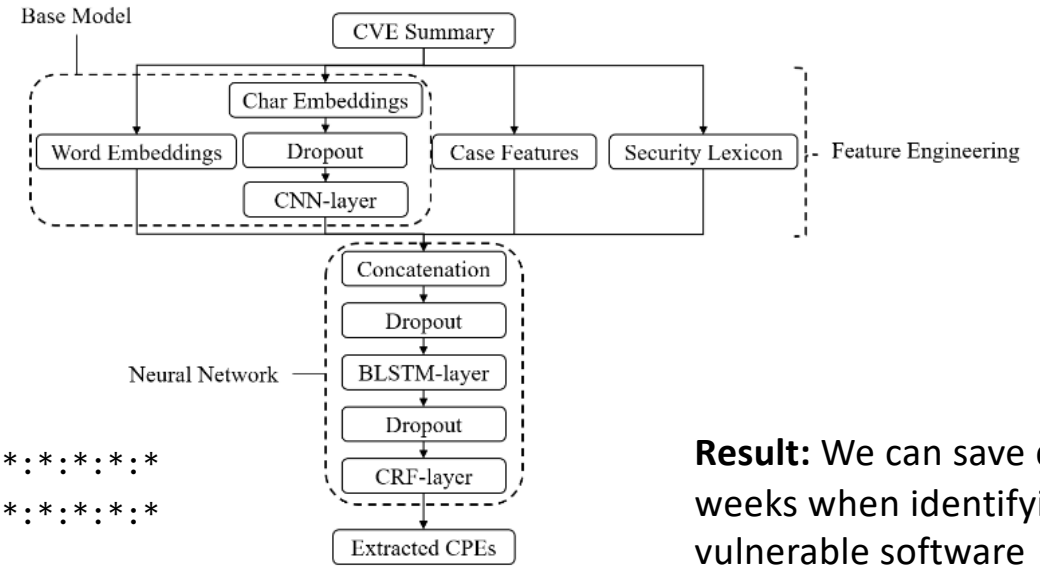
CVE Summary from NVD
Integer overflow in the ProcDRI2GetBuffers function in the DRI2 extension in **X.Org Server** (aka xserver and xorg-server) **before 1.16.3** allows remote authenticated users to cause a denial of service (crash) or possibly execute arbitrary code via a crafted request, which triggers an out-of-bounds read or write.

Delay of days or weeks

Feature engineering

Neural network

…
cpe:2.3:a:x.org:xorg-server:1.16.1:*:*:*:*:*:*:*
cpe:2.3:a:x.org:xorg-server:1.16.2:*:*:*:*:*:*:*
…



Result: We can save days or weeks when identifying new vulnerable software

Text:	extension	in	X.Org	Server	before	1.16.3	allows	remote	authenticated
Label:	O	O	B-product	I-product	O	B-versionEndExcluding	O	O	O