



qazbnm456 / awesome-cve-poc

Watch

169

★ Star

1,040

🍴 Fork

281

<> Code

! Issues 0

🔗 Pull requests 0

📁 Projects 0

📊 Insights

Join GitHub today

GitHub is home to over 20 million developers working together to host and review code, manage projects, and build software together.

Sign up

Dismiss

📌 A curated list of CVE PoCs. <https://awesomelists.top/#/repos/qazbnm456/awesome-cve-poc>

awesome

cve

poc

🕒 412 commits

🔗 1 branch

📦 0 releases

👤 2 contributors

Branch: master ▾

New pull request

Find file

Clone or download ▾





















👤 qazbnm456 add CVE-2018-8897

Latest commit 5a3d203 13 hours ago

📁 .vscode

update CVE-2018-4878

2 months ago

 .gitignore	Create awesome list for cves.	a year ago
 CONTRIBUTING.md	update README.md & CONTRIBUTING.md	2 months ago
 CVE-2017-0070.md	update CVE-2017-5638 & add CVE-2017-0070	a year ago
 CVE-2017-0199.md	update CVE-2017-0199.md	7 months ago
 CVE-2017-0290.md	update	8 months ago
 CVE-2017-0781.md	add CVE-2017-0781	6 months ago
 CVE-2017-1000353.md	add CVE-2017-1000353	10 months ago
 CVE-2017-10271.md	update CVE-2017-10271	a month ago
 CVE-2017-12611.md	update S2-052 and add S2-053	8 months ago
 CVE-2017-16995.md	update CVE-2017-16995	29 days ago
 CVE-2017-5116.md	add CVE-2017-5116 (modified from https://github.com/tunz/js-vuln-db/b...	4 months ago
 CVE-2017-5123.md	add another experiment on CVE-2017-5123	4 months ago
 CVE-2017-5638.md	update CVE-2017-5638	8 months ago
 CVE-2017-5689.md	update CVE-2017-5689	5 months ago
 CVE-2017-5715.md	add one more reference	4 months ago
 CVE-2017-5753.md	add one more reference	4 months ago
 CVE-2017-5754.md	add a repo of POCs for Meltdown Attack	4 months ago
 CVE-2017-7293.md	add CVE-2017-7293	a year ago
 CVE-2017-7494.md	update	8 months ago
 CVE-2017-8464.md	update	8 months ago

 CVE-2017-9791.md	update	8 months ago
 CVE-2017-9805.md	update S2-052 and add S2-053	8 months ago
 CVE-2017-9993.md	update CVE-2017-9993.md	9 months ago
 CVE-2018-0492.md	update CVE-2018-0492	24 days ago
 CVE-2018-0886.md	add CVE-2018-0886	26 days ago
 CVE-2018-4878.md	update CVE-2018-4878	a month ago
 CVE-2018-7600.md	update CVE-2018-7600	18 days ago
 MS17-010.md	add another POC of MS17-010	4 months ago
 README.md	add CVE-2018-8897	13 hours ago
 Stack-Clash.md	update Stack-Clash.md	10 months ago
 code-of-conduct.md	add code-of-conduct.md and revise README.md & CONTRIBUTING.md	10 months ago

README.md

Awesome CVE PoC awesome

 A curated list of CVE PoCs.



Here is a collection about Proof of Concepts of Common Vulnerabilities and Exposures, and you may also want to check out [awesome-web-security](#).

Please read the [contribution guidelines](#) before contributing.

 This repo is full of PoCs for CVEs.

If you enjoy this awesome list and would like to support it, check out my [Patreon](#) page :)
Also, don't forget to check out my [repos](#) 🐾 or say *hi* on my [Twitter](#)!

Contents

- [CVE-2011-2856](#)
- [CVE-2011-3243](#)
- [CVE-2013-2618](#)
- [CVE-2013-6632](#)
- [CVE-2014-1701](#)
- [CVE-2014-1705](#)
- [CVE-2014-3176](#)
- [CVE-2014-6332](#)
- [CVE-2014-7927](#)
- [CVE-2014-7928](#)
- [CVE-2015-0072](#)
- [CVE-2015-0235](#)
- [CVE-2015-0240](#)
- [CVE-2015-1233](#)
- [CVE-2015-1242](#)
- [CVE-2015-1268](#)
- [CVE-2015-1635](#)

- [CVE-2015-1830](#)
- [CVE-2015-3306](#)
- [CVE-2015-5119](#)
- [CVE-2015-5531](#)
- [CVE-2015-6086](#)
- [CVE-2015-6755](#)
- [CVE-2015-6764](#)
- [CVE-2015-6769](#)
- [CVE-2015-6770](#)
- [CVE-2015-6771](#)
- [CVE-2015-7450](#)
- [CVE-2015-7501](#)
- [CVE-2015-7545](#)
- [CVE-2015-8584](#)
- [CVE-2016-0040](#)
- [CVE-2016-0450](#)
- [CVE-2016-0451](#)
- [CVE-2016-0728](#)
- [CVE-2016-0792](#)
- [CVE-2016-1631](#)
- [CVE-2016-1646](#)
- [CVE-2016-1653](#)
- [CVE-2016-1665](#)
- [CVE-2016-1667](#)

- [CVE-2016-1669](#)
- [CVE-2016-1673](#)
- [CVE-2016-1674](#)
- [CVE-2016-1676](#)
- [CVE-2016-1677](#)
- [CVE-2016-1688](#)
- [CVE-2016-1857](#)
- [CVE-2016-1910](#)
- [CVE-2016-2384](#)
- [CVE-2016-2386](#)
- [CVE-2016-2388](#)
- [CVE-2016-3087](#)
- [CVE-2016-3088](#)
- [CVE-2016-3309](#)
- [CVE-2016-3371](#)
- [CVE-2016-3386](#)
- [CVE-2016-4338](#)
- [CVE-2016-4622](#)
- [CVE-2016-4734](#)
- [CVE-2016-4971](#)
- [CVE-2016-5129](#)
- [CVE-2016-5172](#)
- [CVE-2016-5195](#)
- [CVE-2016-5198](#)

- [CVE-2016-5200](#)
- [CVE-2016-5204](#)
- [CVE-2016-5207](#)
- [CVE-2016-5346](#)
- [CVE-2016-5734](#)
- [CVE-2016-6210](#)
- [CVE-2016-6277](#)
- [CVE-2016-6415](#)
- [CVE-2016-6662](#)
- [CVE-2016-6700](#)
- [CVE-2016-6702](#)
- [CVE-2016-6762](#)
- [CVE-2016-6787](#)
- [CVE-2016-7124](#)
- [CVE-2016-7189](#)
- [CVE-2016-7190](#)
- [CVE-2016-7194](#)
- [CVE-2016-7200](#)
- [CVE-2016-7201](#)
- [CVE-2016-7202](#)
- [CVE-2016-7203](#)
- [CVE-2016-7240](#)
- [CVE-2016-7241](#)
- [CVE-2016-7255](#)

- [CVE-2016-7286](#)
- [CVE-2016-7287](#)
- [CVE-2016-7288](#)
- [CVE-2016-7547](#)
- [CVE-2016-7552](#)
- [CVE-2016-8413](#)
- [CVE-2016-8477](#)
- [CVE-2016-8584](#)
- [CVE-2016-8585](#)
- [CVE-2016-8586](#)
- [CVE-2016-8587](#)
- [CVE-2016-8588](#)
- [CVE-2016-8589](#)
- [CVE-2016-8590](#)
- [CVE-2016-8591](#)
- [CVE-2016-8592](#)
- [CVE-2016-8593](#)
- [CVE-2016-9651](#)
- [CVE-2016-9793](#)
- [CVE-2016-10033](#)
- [CVE-2016-10191](#)
- [CVE-2016-10277](#)
- [CVE-2016-10370](#)
- [CVE-2017-0015](#)

- [CVE-2017-0037](#)
- [CVE-2017-0059](#)
- [CVE-2017-0070](#)
- [CVE-2017-0071](#)
- [CVE-2017-0134](#)
- [CVE-2017-0141](#)
- [CVE-2017-0143](#)
- [CVE-2017-0144](#)
- [CVE-2017-0145](#)
- [CVE-2017-0146](#)
- [CVE-2017-0147](#)
- [CVE-2017-0148](#)
- [CVE-2017-0199](#)
- [CVE-2017-0213](#)
- [CVE-2017-0263](#)
- [CVE-2017-0283](#)
- [CVE-2017-0290](#)
- [CVE-2017-0392](#)
- [CVE-2017-0475](#)
- [CVE-2017-0497](#)
- [CVE-2017-0521](#)
- [CVE-2017-0531](#)
- [CVE-2017-0541](#)
- [CVE-2017-0548](#)

- [CVE-2017-0576](#)
- [CVE-2017-0678](#)
- [CVE-2017-0714](#)
- [CVE-2017-0718](#)
- [CVE-2017-0719](#)
- [CVE-2017-0720](#)
- [CVE-2017-0722](#)
- [CVE-2017-0745](#)
- [CVE-2017-0758](#)
- [CVE-2017-0760](#)
- [CVE-2017-0761](#)
- [CVE-2017-0764](#)
- [CVE-2017-0776](#)
- [CVE-2017-0777](#)
- [CVE-2017-0778](#)
- [CVE-2017-0781](#)
- [CVE-2017-0785](#)
- [CVE-2017-0813](#)
- [CVE-2017-0814](#)
- [CVE-2017-0820](#)
- [CVE-2017-1082](#)
- [CVE-2017-1083](#)
- [CVE-2017-1084](#)
- [CVE-2017-1085](#)

- [CVE-2017-2363](#)
- [CVE-2017-2364](#)
- [CVE-2017-2365](#)
- [CVE-2017-2367](#)
- [CVE-2017-2416](#)
- [CVE-2017-2419](#)
- [CVE-2017-2426](#)
- [CVE-2017-2442](#)
- [CVE-2017-2445](#)
- [CVE-2017-2446](#)
- [CVE-2017-2447](#)
- [CVE-2017-2460](#)
- [CVE-2017-2464](#)
- [CVE-2017-2475](#)
- [CVE-2017-2479](#)
- [CVE-2017-2480](#)
- [CVE-2017-2491](#)
- [CVE-2017-2493](#)
- [CVE-2017-2504](#)
- [CVE-2017-2508](#)
- [CVE-2017-2510](#)
- [CVE-2017-2521](#)
- [CVE-2017-2528](#)
- [CVE-2017-2531](#)

- [CVE-2017-2536](#)
- [CVE-2017-2540](#)
- [CVE-2017-2541](#)
- [CVE-2017-2547](#)
- [CVE-2017-2636](#)
- [CVE-2017-2641](#)
- [CVE-2017-3066](#)
- [CVE-2017-3506](#)
- [CVE-2017-3599](#)
- [CVE-2017-3629](#)
- [CVE-2017-3630](#)
- [CVE-2017-3631](#)
- [CVE-2017-3881](#)
- [CVE-2017-4901](#)
- [CVE-2017-4914](#)
- [CVE-2017-4915](#)
- [CVE-2017-4918](#)
- [CVE-2017-4933](#)
- [CVE-2017-4946](#)
- [CVE-2017-4971](#)
- [CVE-2017-5007](#)
- [CVE-2017-5030](#)
- [CVE-2017-5033](#)
- [CVE-2017-5040](#)

- [CVE-2017-5053](#)
- [CVE-2017-5070](#)
- [CVE-2017-5071](#)
- [CVE-2017-5088](#)
- [CVE-2017-5098](#)
- [CVE-2017-5115](#)
- [CVE-2017-5116](#)
- [CVE-2017-5121](#)
- [CVE-2017-5122](#)
- [CVE-2017-5123](#)
- [CVE-2017-5124](#)
- [CVE-2017-5126](#)
- [CVE-2017-5127](#)
- [CVE-2017-5128](#)
- [CVE-2017-5129](#)
- [CVE-2017-5133](#)
- [CVE-2017-5135](#)
- [CVE-2017-5622](#)
- [CVE-2017-5624](#)
- [CVE-2017-5626](#)
- [CVE-2017-5638](#)
- [CVE-2017-5689](#)
- [CVE-2017-5715](#)
- [CVE-2017-5753](#)

- [CVE-2017-5754](#)
- [CVE-2017-5891](#)
- [CVE-2017-5892](#)
- [CVE-2017-5948](#)
- [CVE-2017-6008](#)
- [CVE-2017-6074](#)
- [CVE-2017-6178](#)
- [CVE-2017-6326](#)
- [CVE-2017-6327](#)
- [CVE-2017-6736](#)
- [CVE-2017-6980](#)
- [CVE-2017-6984](#)
- [CVE-2017-7037](#)
- [CVE-2017-7056](#)
- [CVE-2017-7061](#)
- [CVE-2017-7089](#)
- [CVE-2017-7092](#)
- [CVE-2017-7115](#)
- [CVE-2017-7117](#)
- [CVE-2017-7219](#)
- [CVE-2017-7269](#)
- [CVE-2017-7279](#)
- [CVE-2017-7280](#)
- [CVE-2017-7281](#)

- [CVE-2017-7281](#)
- [CVE-2017-7281](#)
- [CVE-2017-7293](#)
- [CVE-2017-7308](#)
- [CVE-2017-7344](#)
- [CVE-2017-7442](#)
- [CVE-2017-7494](#)
- [CVE-2017-7504](#)
- [CVE-2017-7525](#)
- [CVE-2017-7529](#)
- [CVE-2017-7533](#)
- [CVE-2017-8046](#)
- [CVE-2017-8295](#)
- [CVE-2017-8386](#)
- [CVE-2017-8464](#)
- [CVE-2017-8514](#)
- [CVE-2017-8543](#)
- [CVE-2017-8548](#)
- [CVE-2017-8570](#)
- [CVE-2017-8601](#)
- [CVE-2017-8625](#)
- [CVE-2017-8634](#)
- [CVE-2017-8636](#)
- [CVE-2017-8640](#)

- [CVE-2017-8645](#)
- [CVE-2017-8646](#)
- [CVE-2017-8656](#)
- [CVE-2017-8670](#)
- [CVE-2017-8671](#)
- [CVE-2017-8729](#)
- [CVE-2017-8740](#)
- [CVE-2017-8751](#)
- [CVE-2017-8755](#)
- [CVE-2017-8759](#)
- [CVE-2017-8817](#)
- [CVE-2017-8850](#)
- [CVE-2017-8851](#)
- [CVE-2017-8877](#)
- [CVE-2017-8878](#)
- [CVE-2017-8890](#)
- [CVE-2017-8912](#)
- [CVE-2017-8917](#)
- [CVE-2017-9417](#)
- [CVE-2017-9791](#)
- [CVE-2017-9798](#)
- [CVE-2017-9805](#)
- [CVE-2017-9822](#)
- [CVE-2017-9948](#)

- [CVE-2017-9993](#)
- [CVE-2017-10271](#)
- [CVE-2017-10661](#)
- [CVE-2017-11105](#)
- [CVE-2017-11120](#)
- [CVE-2017-11421](#)
- [CVE-2017-11444](#)
- [CVE-2017-11610](#)
- [CVE-2017-11764](#)
- [CVE-2017-11774](#)
- [CVE-2017-11779](#)
- [CVE-2017-11793](#)
- [CVE-2017-11799](#)
- [CVE-2017-11802](#)
- [CVE-2017-11809](#)
- [CVE-2017-11811](#)
- [CVE-2017-11812](#)
- [CVE-2017-11839](#)
- [CVE-2017-11840](#)
- [CVE-2017-11841](#)
- [CVE-2017-11855](#)
- [CVE-2017-11861](#)
- [CVE-2017-11870](#)
- [CVE-2017-11873](#)

- [CVE-2017-11882](#)
- [CVE-2017-11890](#)
- [CVE-2017-11893](#)
- [CVE-2017-11903](#)
- [CVE-2017-11906](#)
- [CVE-2017-11907](#)
- [CVE-2017-11909](#)
- [CVE-2017-11911](#)
- [CVE-2017-11914](#)
- [CVE-2017-11918](#)
- [CVE-2017-12097](#)
- [CVE-2017-12098](#)
- [CVE-2017-12149](#)
- [CVE-2017-12542](#)
- [CVE-2017-12581](#)
- [CVE-2017-12611](#)
- [CVE-2017-12615](#)
- [CVE-2017-12617](#)
- [CVE-2017-13089](#)
- [CVE-2017-13253](#)
- [CVE-2017-13258](#)
- [CVE-2017-13260](#)
- [CVE-2017-13261](#)
- [CVE-2017-13262](#)

- [CVE-2017-13791](#)
- [CVE-2017-13792](#)
- [CVE-2017-14335](#)
- [CVE-2017-14491](#)
- [CVE-2017-14492](#)
- [CVE-2017-14493](#)
- [CVE-2017-14494](#)
- [CVE-2017-14495](#)
- [CVE-2017-14496](#)
- [CVE-2017-14904](#)
- [CVE-2017-15303](#)
- [CVE-2017-15361](#)
- [CVE-2017-15388](#)
- [CVE-2017-15396](#)
- [CVE-2017-15398](#)
- [CVE-2017-15399](#)
- [CVE-2017-15401](#)
- [CVE-2017-15411](#)
- [CVE-2017-15412](#)
- [CVE-2017-15415](#)
- [CVE-2017-15428](#)
- [CVE-2017-15613](#)
- [CVE-2017-15614](#)
- [CVE-2017-15615](#)

- [CVE-2017-15616](#)
- [CVE-2017-15617](#)
- [CVE-2017-15618](#)
- [CVE-2017-15619](#)
- [CVE-2017-15620](#)
- [CVE-2017-15621](#)
- [CVE-2017-15622](#)
- [CVE-2017-15623](#)
- [CVE-2017-15624](#)
- [CVE-2017-15625](#)
- [CVE-2017-15626](#)
- [CVE-2017-15627](#)
- [CVE-2017-15628](#)
- [CVE-2017-15629](#)
- [CVE-2017-15630](#)
- [CVE-2017-15631](#)
- [CVE-2017-15632](#)
- [CVE-2017-15633](#)
- [CVE-2017-15634](#)
- [CVE-2017-15635](#)
- [CVE-2017-15636](#)
- [CVE-2017-15637](#)
- [CVE-2017-15944](#)
- [CVE-2017-16544](#)

- [CVE-2017-16584](#)
- [CVE-2017-16716](#)
- [CVE-2017-16943](#)
- [CVE-2017-16944](#)
- [CVE-2017-16995](#)
- [CVE-2017-17033](#)
- [CVE-2017-17107](#)
- [CVE-2017-17215](#)
- [CVE-2017-17405](#)
- [CVE-2017-17562](#)
- [CVE-2017-17692](#)
- [CVE-2017-17867](#)
- [CVE-2017-17969](#)
- [CVE-2017-1000112](#)
- [CVE-2017-1000117](#)
- [CVE-2017-1000251](#)
- [CVE-2017-1000353](#)
- [CVE-2017-1000364](#)
- [CVE-2017-1000365](#)
- [CVE-2017-1000366](#)
- [CVE-2017-1000367](#)
- [CVE-2017-1000369](#)
- [CVE-2017-1000370](#)
- [CVE-2017-1000371](#)

- [CVE-2017-1000372](#)
- [CVE-2017-1000373](#)
- [CVE-2017-1000374](#)
- [CVE-2017-1000375](#)
- [CVE-2017-1000376](#)
- [CVE-2017-1000377](#)
- [CVE-2017-1000378](#)
- [CVE-2017-1000379](#)
- [CVE-2017-1000405](#)
- [CVE-2017-1000424](#)
- [CVE-2017-1000459](#)
- [CVE-2017-1002101](#)
- [CVE-2018-0101](#)
- [CVE-2018-0114](#)
- [CVE-2018-0171](#)
- [CVE-2018-0492](#)
- [CVE-2018-0743](#)
- [CVE-2018-0744](#)
- [CVE-2018-0752](#)
- [CVE-2018-0758](#)
- [CVE-2018-0763](#)
- [CVE-2018-0767](#)
- [CVE-2018-0769](#)
- [CVE-2018-0770](#)

- [CVE-2018-0774](#)
- [CVE-2018-0775](#)
- [CVE-2018-0776](#)
- [CVE-2018-0777](#)
- [CVE-2018-0780](#)
- [CVE-2018-0797](#)
- [CVE-2018-0802](#)
- [CVE-2018-0833](#)
- [CVE-2018-0834](#)
- [CVE-2018-0835](#)
- [CVE-2018-0837](#)
- [CVE-2018-0838](#)
- [CVE-2018-0840](#)
- [CVE-2018-0860](#)
- [CVE-2018-0878](#)
- [CVE-2018-0886](#)
- [CVE-2018-0891](#)
- [CVE-2018-0933](#)
- [CVE-2018-0934](#)
- [CVE-2018-1037](#)
- [CVE-2018-1038](#)
- [CVE-2018-1270](#)
- [CVE-2018-1273](#)
- [CVE-2018-1275](#)

- [CVE-2018-2628](#)
- [CVE-2018-2694](#)
- [CVE-2018-2698](#)
- [CVE-2018-4087](#)
- [CVE-2018-4121](#)
- [CVE-2018-4148](#)
- [CVE-2018-4150](#)
- [CVE-2018-4878](#)
- [CVE-2018-5146](#)
- [CVE-2018-5181](#)
- [CVE-2018-5189](#)
- [CVE-2018-5318](#)
- [CVE-2018-5711](#)
- [CVE-2018-5996](#)
- [CVE-2018-6034](#)
- [CVE-2018-6055](#)
- [CVE-2018-6072](#)
- [CVE-2018-6184](#)
- [CVE-2018-6317](#)
- [CVE-2018-6376](#)
- [CVE-2018-6389](#)
- [CVE-2018-6460](#)
- [CVE-2018-6789](#)
- [CVE-2018-6794](#)

- [CVE-2018-6871](#)
- [CVE-2018-7260](#)
- [CVE-2018-7273](#)
- [CVE-2018-7600](#)
- [CVE-2018-7602](#)
- [CVE-2018-8719](#)
- [CVE-2018-8733](#)
- [CVE-2018-8734](#)
- [CVE-2018-8735](#)
- [CVE-2018-8736](#)
- [CVE-2018-8778](#)
- [CVE-2018-8897](#)
- [CVE-2018-9995](#)
- [CVE-2018-10115](#)
- [CVE-2018-10172](#)
- [CVE-2018-10561](#)
- [CVE-2018-10562](#)
- [CVE-2018-10641](#)
- [CVE-2018-10676](#)
- [CVE-2018-1000006](#)
- [CVE-2018-1000129](#)
- [CVE-2018-1000130](#)
- [CVE-2018-1000136](#)

Resource

CVE-2011-2856

- Google V8, as used in Google Chrome before 14.0.835.163, allows remote attackers to bypass the Same Origin Policy via unspecified vectors.

CVE-2011-3243

- Cross-site scripting (XSS) vulnerability in WebKit, as used in Apple iOS before 5 and Safari before 5.1.1, allows remote attackers to inject arbitrary web script or HTML via vectors involving inactive DOM windows.

CVE-2013-2618

- Cross-site scripting (XSS) vulnerability in editor.php in Network Weathermap before 0.97b allows remote attackers to inject arbitrary web script or HTML via the map_title parameter.

CVE-2013-6632

- Integer overflow in Google Chrome before 31.0.1650.57 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, as demonstrated during a Mobile Pwn2Own competition at PacSec 2013.

CVE-2014-1701

- The GenerateFunction function in bindings/scripts/code_generator_v8.pm in Blink, as used in Google Chrome before 33.0.1750.149, does not implement a certain cross-origin restriction for the EventTarget::dispatchEvent function, which allows remote attackers to conduct Universal XSS (UXSS) attacks via vectors involving events.

CVE-2014-1705

- Google V8, as used in Google Chrome before 33.0.1750.152 on OS X and Linux and before 33.0.1750.154 on Windows, allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.

CVE-2014-3176

- Google Chrome before 37.0.2062.94 does not properly handle the interaction of extensions, IPC, the sync API, and Google V8, which allows remote attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2014-3177.

CVE-2014-6332

- OleAut32.dll in OLE in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows remote attackers to execute arbitrary code via a crafted web site, as demonstrated by an array-redimensioning attempt that triggers improper handling of a size value in the SafeArrayDimen function, aka "Windows OLE Automation Array Remote Code Execution Vulnerability."

CVE-2014-7927

- The SimplifiedLowering::DoLoadBuffer function in compiler/simplified-lowering.cc in Google V8, as used in Google Chrome before 40.0.2214.91, does not properly choose an integer data type, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via crafted JavaScript code.

CVE-2014-7928

- hydrogen.cc in Google V8, as used Google Chrome before 40.0.2214.91, does not properly handle arrays with holes, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via crafted JavaScript code that triggers an array copy.

CVE-2015-0072

- Cross-site scripting (XSS) vulnerability in Microsoft Internet Explorer 9 through 11 allows remote attackers to bypass the Same Origin Policy and inject arbitrary web script or HTML via vectors involving an IFRAME element that triggers a redirect, a second IFRAME element that does not trigger a redirect, and an eval of a WindowProxy object, aka "Universal XSS (UXSS)."

CVE-2015-0235

- Heap-based buffer overflow in the `__nss_hostname_digits_dots` function in glibc 2.2, and other 2.x versions before 2.18, allows context-dependent attackers to execute arbitrary code via vectors related to the (1) `gethostbyname` or (2) `gethostbyname2` function, aka "GHOST".

CVE-2015-0240

- The Netlogon server implementation in `smbd` in Samba 3.5.x and 3.6.x before 3.6.25, 4.0.x before 4.0.25, 4.1.x before 4.1.17, and 4.2.x before 4.2.0rc5 performs a free operation on an uninitialized stack pointer, which allows remote attackers to execute arbitrary code via crafted Netlogon packets that use the `ServerPasswordSet` RPC API, as demonstrated by packets reaching the `_netr_ServerPasswordSet` function in `rpc_server/netlogon/srv_netlog_nt.c`.

CVE-2015-1233

- Google Chrome before 41.0.2272.118 does not properly handle the interaction of IPC, the Gamepad API, and Google V8, which allows remote attackers to execute arbitrary code via unspecified vectors.

CVE-2015-1242

- The ReduceTransitionElementsKind function in hydrogen-check-elimination.cc in Google V8 before 4.2.77.8, as used in Google Chrome before 42.0.2311.90, allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted JavaScript code that leverages "type confusion" in the check-elimination optimization.

CVE-2015-1268

- bindings/scripts/v8_types.py in Blink, as used in Google Chrome before 43.0.2357.130, does not properly select a creation context for a return value's DOM wrapper, which allows remote attackers to bypass the Same Origin Policy via crafted JavaScript code, as demonstrated by use of a data: URL.

CVE-2015-1635

- HTTP.sys in Microsoft Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8, Windows 8.1, and Windows Server 2012 Gold and R2 allows remote attackers to execute arbitrary code via crafted HTTP requests, aka "HTTP.sys Remote Code Execution Vulnerability."

CVE-2015-1830

- Directory traversal vulnerability in the fileserver upload/download functionality for blob messages in Apache ActiveMQ 5.x before 5.11.2 for Windows allows remote attackers to create JSP files in arbitrary directories via unspecified vectors.

CVE-2015-3306

- The mod_copy module in ProFTPD 1.3.5 allows remote attackers to read and write to arbitrary files via the site cpfr and site cpto commands.

CVE-2015-5119

- Use-after-free vulnerability in the ByteArray class in the ActionScript 3 (AS3) implementation in Adobe Flash Player 13.x through 13.0.0.296 and 14.x through 18.0.0.194 on Windows and OS X and 11.x through 11.2.202.468 on Linux allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via crafted Flash content that overrides a valueOf function, as exploited in the wild in July 2015.

CVE-2015-5531

- Directory traversal vulnerability in Elasticsearch before 1.6.1 allows remote attackers to read arbitrary files via unspecified vectors related to snapshot API calls.

CVE-2015-6086

- Microsoft Internet Explorer 9 through 11 allows remote attackers to obtain sensitive information from process memory via a crafted web site, aka "Internet Explorer Information Disclosure Vulnerability."

CVE-2015-6755

- The ContainerNode::parserInsertBefore function in core/dom/ContainerNode.cpp in Blink, as used in Google Chrome before 46.0.2490.71, proceeds with a DOM tree insertion in certain cases where a parent node no longer contains a child node, which allows remote attackers to bypass the Same Origin Policy via crafted JavaScript code.

CVE-2015-6764

- The BasicJsonStringifier::SerializeJSArray function in json-stringifier.h in the JSON stringifier in Google V8, as used in Google Chrome before 47.0.2526.73, improperly loads array elements, which allows remote attackers to cause a denial of service (out-of-bounds memory access) or possibly have unspecified other impact via crafted JavaScript code.

CVE-2015-6769

- The provisional-load commit implementation in WebKit/Source/bindings/core/v8/WindowProxy.cpp in Google Chrome before 47.0.2526.73 allows remote attackers to bypass the Same Origin Policy by leveraging a delay in window proxy clearing.

CVE-2015-6770

- The DOM implementation in Google Chrome before 47.0.2526.73 allows remote attackers to bypass the Same Origin Policy via unspecified vectors, a different vulnerability than CVE-2015-6768.

CVE-2015-6771

- js/array.js in Google V8, as used in Google Chrome before 47.0.2526.73, improperly implements certain map and filter operations for arrays, which allows remote attackers to cause a denial of service (out-of-bounds memory access) or possibly have unspecified other impact via crafted JavaScript code.

CVE-2015-7450

- Serialized-object interfaces in certain IBM analytics, business solutions, cognitive, IT infrastructure, and mobile and social products allow remote attackers to execute arbitrary commands via a crafted serialized Java object, related to the InvokerTransformer class in the Apache Commons Collections library.

CVE-2015-7501

- Red Hat JBoss A-MQ 6.x; BPM Suite (BPMS) 6.x; BRMS 6.x and 5.x; Data Grid (JDG) 6.x; Data Virtualization (JDV) 6.x and 5.x; Enterprise Application Platform 6.x, 5.x, and 4.3.x; Fuse 6.x; Fuse Service Works (FSW) 6.x; Operations Network (JBoss ON) 3.x; Portal 6.x; SOA Platform (SOA-P) 5.x; Web Server (JWS) 3.x; Red Hat OpenShift/xPAAS 3.x; and Red Hat Subscription Asset Manager 1.3 allow remote attackers to execute arbitrary commands via a crafted serialized Java object, related to the Apache Commons Collections (ACC) library.

CVE-2015-7545

- The (1) git-remote-ext and (2) unspecified other remote helper programs in Git before 2.3.10, 2.4.x before 2.4.10, 2.5.x before 2.5.4, and 2.6.x before 2.6.1 do not properly restrict the allowed protocols, which might allow remote attackers to execute arbitrary code via a URL in a (a) .gitmodules file or (b) unknown other sources in a submodule.

CVE-2015-8584

- JSON, OOB.

CVE-2016-0040

- The kernel in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 allows local users to gain privileges via a crafted application, aka "Windows Elevation of Privilege Vulnerability."

CVE-2016-0450

- Unspecified vulnerability in the Oracle GoldenGate component in Oracle GoldenGate 11.2 and 12.1.2 allows remote attackers to affect availability via unknown vectors.

CVE-2016-0451

- Unspecified vulnerability in the Oracle GoldenGate component in Oracle GoldenGate 11.2 and 12.1.2 allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors, a different vulnerability than CVE-2016-0452.

CVE-2016-0728

- The join_session_keyring function in security/keys/process_keys.c in the Linux kernel before 4.4.1 mishandles object references in a certain error case, which allows local users to gain privileges or cause a denial of service (integer

overflow and use-after-free) via crafted keyctl commands.

CVE-2016-0792

- Multiple unspecified API endpoints in Jenkins before 1.650 and LTS before 1.642.2 allow remote authenticated users to execute arbitrary code via serialized data in an XML file, related to XStream and groovy.util.Expando.

CVE-2016-1631

- The PPB_Flash_MessageLoop_Impl::InternalRun function in content/renderer/pepper/ppb_flash_message_loop_impl.cc in the Pepper plugin in Google Chrome before 49.0.2623.75 mishandles nested message loops, which allows remote attackers to bypass the Same Origin Policy via a crafted web site.

CVE-2016-1646

- The Array.prototype.concat implementation in builtins.cc in Google V8, as used in Google Chrome before 49.0.2623.108, does not properly consider element data types, which allows remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact via crafted JavaScript code.

CVE-2016-1653

- The LoadBuffer implementation in Google V8, as used in Google Chrome before 50.0.2661.75, mishandles data types, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted JavaScript code that triggers an out-of-bounds write operation, related to compiler/pipeline.cc and compiler/simplified-lowering.cc.

CVE-2016-1665

- The JSGenericLowering class in compiler/js-generic-lowering.cc in Google V8, as used in Google Chrome before 50.0.2661.94, mishandles comparison operators, which allows remote attackers to obtain sensitive information via crafted JavaScript code.

CVE-2016-1667

- The TreeScope::adoptIfNeeded function in WebKit/Source/core/dom/TreeScope.cpp in the DOM implementation in Blink, as used in Google Chrome before 50.0.2661.102, does not prevent script execution during node-adoption operations, which allows remote attackers to bypass the Same Origin Policy via a crafted web site.

CVE-2016-1669

- The Zone::New function in zone.cc in Google V8 before 5.0.71.47, as used in Google Chrome before 50.0.2661.102, does not properly determine when to expand certain memory allocations, which allows remote attackers to cause a denial of service (buffer overflow) or possibly have unspecified other impact via crafted JavaScript code.

CVE-2016-1673

- Blink, as used in Google Chrome before 51.0.2704.63, allows remote attackers to bypass the Same Origin Policy via unspecified vectors.

CVE-2016-1674

- The extensions subsystem in Google Chrome before 51.0.2704.63 allows remote attackers to bypass the Same Origin Policy via unspecified vectors.

CVE-2016-1676

- `extensions/renderer/resources/binding.js` in the extension bindings in Google Chrome before 51.0.2704.63 does not properly use prototypes, which allows remote attackers to bypass the Same Origin Policy via unspecified vectors.

CVE-2016-1677

- `uri.js` in Google V8 before 5.1.281.26, as used in Google Chrome before 51.0.2704.63, uses an incorrect array type, which allows remote attackers to obtain sensitive information by calling the `decodeURI` function and leveraging "type confusion".

CVE-2016-1688

- The regexp (aka regular expression) implementation in Google V8 before 5.0.71.40, as used in Google Chrome before 51.0.2704.63, mishandles external string sizes, which allows remote attackers to cause a denial of service (out-of-bounds read) via crafted JavaScript code.

CVE-2016-1857

- WebKit, as used in Apple iOS before 9.3.2, Safari before 9.1.1, and tvOS before 9.2.1, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, a different vulnerability than CVE-2016-1854, CVE-2016-1855, and CVE-2016-1856.

CVE-2016-1910

- The User Management Engine (UME) in SAP NetWeaver 7.4 allows attackers to decrypt unspecified data via unknown vectors, aka SAP Security Note 2191290.

CVE-2016-2384

- Double free vulnerability in the `snd_usbmidi_create` function in `sound/usb/midi.c` in the Linux kernel before 4.5 allows physically proximate attackers to cause a denial of service (panic) or possibly have unspecified other impact via vectors involving an invalid USB descriptor.

CVE-2016-2386

- SQL injection vulnerability in the UDDI server in SAP NetWeaver J2EE Engine 7.40 allows remote attackers to execute arbitrary SQL commands via unspecified vectors, aka SAP Security Note 2101079.

CVE-2016-2388

- The Universal Worklist Configuration in SAP NetWeaver 7.4 allows remote attackers to obtain sensitive user information via a crafted HTTP request, aka SAP Security Note 2256846.

CVE-2016-3087

- Apache Struts 2.3.20.x before 2.3.20.3, 2.3.24.x before 2.3.24.3, and 2.3.28.x before 2.3.28.1, when Dynamic Method Invocation is enabled, allow remote attackers to execute arbitrary code via vectors related to an `!` (exclamation mark) operator to the REST Plugin.

CVE-2016-3088

- The Fileserver web application in Apache ActiveMQ 5.x before 5.14.0 allows remote attackers to upload and execute arbitrary files via an HTTP PUT followed by an HTTP MOVE request.

CVE-2016-3309

- The kernel-mode drivers in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT 8.1; and Windows 10 Gold, 1511, and 1607 allow local

users to gain privileges via a crafted application, aka "Win32k Elevation of Privilege Vulnerability," a different vulnerability than CVE-2016-3308, CVE-2016-3310, and CVE-2016-3311.

CVE-2016-3371

- The kernel API in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold, 1511, and 1607 does not properly enforce permissions, which allows local users to obtain sensitive information via a crafted application, aka "Windows Kernel Elevation of Privilege Vulnerability."

CVE-2016-3386

- The Chakra JavaScript engine in Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability," a different vulnerability than CVE-2016-3389, CVE-2016-7190, and CVE-2016-7194.

CVE-2016-4338

- The mysql user parameter configuration script (userparameter_mysql.conf) in the agent in Zabbix before 2.0.18, 2.2.x before 2.2.13, and 3.0.x before 3.0.3, when used with a shell other than bash, allows context-dependent attackers to execute arbitrary code or SQL commands via the mysql.size parameter.

CVE-2016-4622

- WebKit in Apple iOS before 9.3.3, Safari before 9.1.2, and tvOS before 9.2.2 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, a different vulnerability than CVE-2016-4589, CVE-2016-4623, and CVE-2016-4624.

CVE-2016-4734

- WebKit in Apple iOS before 10, Safari before 10, and tvOS before 10 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, a different vulnerability than CVE-2016-4611, CVE-2016-4730, CVE-2016-4733, and CVE-2016-4735.

CVE-2016-4971

- GNU wget before 1.18 allows remote servers to write to arbitrary files by redirecting a request from HTTP to a crafted FTP resource.

CVE-2016-5129

- Google V8 before 5.2.361.32, as used in Google Chrome before 52.0.2743.82, does not properly process left-trimmed objects, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via crafted JavaScript code.

CVE-2016-5172

- The parser in Google V8, as used in Google Chrome before 53.0.2785.113, mishandles scopes, which allows remote attackers to obtain sensitive information from arbitrary memory locations via crafted JavaScript code.

CVE-2016-5195

- Race condition in mm/gup.c in the Linux kernel 2.x through 4.x before 4.8.3 allows local users to gain privileges by leveraging incorrect handling of a copy-on-write (COW) feature to write to a read-only memory mapping, as exploited in the wild in October 2016, aka "Dirty COW."

CVE-2016-5198

- V8 in Google Chrome prior to 54.0.2840.90 for Linux, and 54.0.2840.85 for Android, and 54.0.2840.87 for Windows and Mac included incorrect optimisation assumptions, which allowed a remote attacker to perform arbitrary read/write operations, leading to code execution, via a crafted HTML page.

CVE-2016-5200

- V8 in Google Chrome prior to 54.0.2840.98 for Mac, and 54.0.2840.99 for Windows, and 54.0.2840.100 for Linux, and 55.0.2883.84 for Android incorrectly applied type rules, which allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.

CVE-2016-5204

- Leaking of an SVG shadow tree leading to corruption of the DOM tree in Blink in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android allowed a remote attacker to inject arbitrary scripts or HTML (UXSS) via a crafted HTML page.

CVE-2016-5207

- In Blink in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android, corruption of the DOM tree could occur during the removal of a full screen element, which allowed a remote attacker to achieve arbitrary code execution via a crafted HTML page.

CVE-2016-5346

- ** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.

CVE-2016-5734

- phpMyAdmin 4.0.x before 4.0.10.16, 4.4.x before 4.4.15.7, and 4.6.x before 4.6.3 does not properly choose delimiters to prevent use of the preg_replace e (aka eval) modifier, which might allow remote attackers to execute arbitrary PHP code via a crafted string, as demonstrated by the table search-and-replace implementation.

CVE-2016-6210

- sshd in OpenSSH before 7.3, when SHA256 or SHA512 are used for user password hashing, uses BLOWFISH hashing on a static password when the username does not exist, which allows remote attackers to enumerate users by leveraging the timing difference between responses when a large password is provided.

CVE-2016-6277

- NETGEAR R6250 before 1.0.4.6.Beta, R6400 before 1.0.1.18.Beta, R6700 before 1.0.1.14.Beta, R6900, R7000 before 1.0.7.6.Beta, R7100LG before 1.0.0.28.Beta, R7300DST before 1.0.0.46.Beta, R7900 before 1.0.1.8.Beta, R8000 before 1.0.3.26.Beta, D6220, D6400, D7000, and possibly other routers allow remote attackers to execute arbitrary commands via shell metacharacters in the path info to cgi-bin/.

CVE-2016-6415

- The server IKEv1 implementation in Cisco IOS 12.2 through 12.4 and 15.0 through 15.6, IOS XE through 3.18S, IOS XR 4.3.x and 5.0.x through 5.2.x, and PIX before 7.0 allows remote attackers to obtain sensitive information from device memory via a Security Association (SA) negotiation request, aka Bug IDs CSCvb29204 and CSCvb36055 or BENIGNCERTAIN.

CVE-2016-6662

- Oracle MySQL through 5.5.52, 5.6.x through 5.6.33, and 5.7.x through 5.7.15; MariaDB before 5.5.51, 10.0.x before 10.0.27, and 10.1.x before 10.1.17; and Percona Server before 5.5.51-38.1, 5.6.x before 5.6.32-78.0, and 5.7.x before 5.7.14-7 allow local users to create arbitrary configurations and bypass certain protection mechanisms by setting

general_log_file to a my.cnf configuration. NOTE: this can be leveraged to execute arbitrary code with root privileges by setting malloc_lib. NOTE: the affected MySQL version information is from Oracle's October 2016 CPU. Oracle has not commented on third-party claims that the issue was silently patched in MySQL 5.5.52, 5.6.33, and 5.7.15.

CVE-2016-6700

- An elevation of privilege vulnerability in libzipfile in Android 4.x before 4.4.4, 5.0.x before 5.0.2, and 5.1.x before 5.1.1 could enable a local malicious application to execute arbitrary code within the context of a privileged process. This issue is rated as Critical due to the possibility of a local permanent device compromise, which may require reflashing the operating system to repair the device. Android ID: A-30916186.

CVE-2016-6702

- A remote code execution vulnerability in libjpeg in Android 4.x before 4.4.4, 5.0.x before 5.0.2, and 5.1.x before 5.1.1 could enable an attacker using a specially crafted file to execute arbitrary code in the context of an unprivileged process. This issue is rated as High due to the possibility of remote code execution in an application that uses libjpeg. Android ID: A-30259087.

CVE-2016-6762

- An elevation of privilege vulnerability in the libziparchive library could enable a local malicious application to execute arbitrary code within the context of a privileged process. This issue is rated as High because it could be used to gain local access to elevated capabilities, which are not normally accessible to a third-party application. Product: Android. Versions: 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0. Android ID: A-31251826.

CVE-2016-6787

- kernel/events/core.c in the performance subsystem in the Linux kernel before 4.0 mismanages locks during certain migrations, which allows local users to gain privileges via a crafted application, aka Android internal bug 31095224.

CVE-2016-7124

- ext/standard/var_unserializer.c in PHP before 5.6.25 and 7.x before 7.0.10 mishandles certain invalid objects, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted serialized data that leads to a (1) __destruct call or (2) magic method call.

CVE-2016-7189

- The Chakra JavaScript engine in Microsoft Edge allows remote attackers to execute arbitrary code via a crafted web site, aka "Scripting Engine Remote Code Execution Vulnerability".

CVE-2016-7190

- The Chakra JavaScript engine in Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability," a different vulnerability than CVE-2016-3386, CVE-2016-3389, and CVE-2016-7194.

CVE-2016-7194

- The Chakra JavaScript engine in Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability," a different vulnerability than CVE-2016-3386, CVE-2016-3389, and CVE-2016-7190.

CVE-2016-7200

- The Chakra JavaScript scripting engine in Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability," a different vulnerability than CVE-2016-7201, CVE-2016-7202, CVE-2016-7203, CVE-2016-7208, CVE-2016-7240, CVE-2016-7242, and CVE-2016-7243.

CVE-2016-7201

- The Chakra JavaScript scripting engine in Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability," a different vulnerability than CVE-2016-7200, CVE-2016-7202, CVE-2016-7203, CVE-2016-7208, CVE-2016-7240, CVE-2016-7242, and CVE-2016-7243.

CVE-2016-7202

- The scripting engines in Microsoft Internet Explorer 9 through 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability," as demonstrated by the Chakra JavaScript engine, a different vulnerability than CVE-2016-7200, CVE-2016-7201, CVE-2016-7203, CVE-2016-7208, CVE-2016-7240, CVE-2016-7242, and CVE-2016-7243.

CVE-2016-7203

- The Chakra JavaScript scripting engine in Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability," a different vulnerability than CVE-2016-7200, CVE-2016-7201, CVE-2016-7202, CVE-2016-7208, CVE-2016-7240, CVE-2016-7242, and CVE-2016-7243.

CVE-2016-7240

- The Chakra JavaScript scripting engine in Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability," a different vulnerability than CVE-2016-7200, CVE-2016-7201, CVE-2016-7202, CVE-2016-7203, CVE-2016-7208, CVE-2016-7242, and CVE-2016-7243.

CVE-2016-7241

- Microsoft Internet Explorer 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Memory Corruption Vulnerability".

CVE-2016-7255

- The kernel-mode drivers in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, and 1607, and Windows Server 2016 allow local users to gain privileges via a crafted application, aka "Win32k Elevation of Privilege Vulnerability."

CVE-2016-7286

- The scripting engines in Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability," a different vulnerability than CVE-2016-7288, CVE-2016-7296, and CVE-2016-7297.

CVE-2016-7287

- The scripting engines in Microsoft Internet Explorer 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability".

CVE-2016-7288

- The scripting engines in Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability," a different vulnerability than CVE-2016-7286, CVE-2016-7296, and CVE-2016-7297.

CVE-2016-7547

- A command execution flaw on the Trend Micro Threat Discovery Appliance 2.6.1062r1 exists with the timezone parameter in the admin_sys_time.cgi interface.

CVE-2016-7552

- On the Trend Micro Threat Discovery Appliance 2.6.1062r1, directory traversal when processing a session_id cookie allows a remote, unauthenticated attacker to delete arbitrary files as root. This can be used to bypass authentication or cause a DoS.

CVE-2016-8413

- An information disclosure vulnerability in the Qualcomm camera driver could enable a local malicious application to access data outside of its permission levels. This issue is rated as Moderate because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A-32709702. References: QC-CR#518731.

CVE-2016-8477

- An information disclosure vulnerability in the Qualcomm camera driver could enable a local malicious application to access data outside of its permission levels. This issue is rated as Moderate because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A-32720522. References: QC-CR#1090007.

CVE-2016-8584

- Trend Micro Threat Discovery Appliance 2.6.1062r1 and earlier uses predictable session values, which allows remote attackers to bypass authentication by guessing the value.

CVE-2016-8585

- `admin_sys_time.cgi` in Trend Micro Threat Discovery Appliance 2.6.1062r1 and earlier allows remote authenticated users to execute arbitrary code as the root user via shell metacharacters in the `timezone` parameter.

CVE-2016-8586

- `detected_potential_files.cgi` in Trend Micro Threat Discovery Appliance 2.6.1062r1 and earlier allows remote authenticated users to execute arbitrary code as the root user via shell metacharacters in the `cache_id` parameter.

CVE-2016-8587

- `dlp_policy_upload.cgi` in Trend Micro Threat Discovery Appliance 2.6.1062r1 and earlier allows remote authenticated users to execute arbitrary code via an archive file containing a symlink to `/eng_ptn_stores/prod/sensorSDK/data/` or `/eng_ptn_stores/prod/sensorSDK/backup_pol/`.

CVE-2016-8588

- The `hotfix_upload.cgi` in Trend Micro Threat Discovery Appliance 2.6.1062r1 and earlier allows remote authenticated users to execute arbitrary code via shell metacharacters in the file name of an uploaded file.

CVE-2016-8589

- `log_query_dae.cgi` in Trend Micro Threat Discovery Appliance 2.6.1062r1 and earlier allows remote authenticated users to execute arbitrary code as the root user via shell metacharacters in the `cache_id` parameter.

CVE-2016-8590

- `log_query_dlp.cgi` in Trend Micro Threat Discovery Appliance 2.6.1062r1 and earlier allows remote authenticated users to execute arbitrary code as the root user via shell metacharacters in the `cache_id` parameter.

CVE-2016-8591

- log_query.cgi in Trend Micro Threat Discovery Appliance 2.6.1062r1 and earlier allows remote authenticated users to execute arbitrary code as the root user via shell metacharacters in the cache_id parameter.

CVE-2016-8592

- log_query_system.cgi in Trend Micro Threat Discovery Appliance 2.6.1062r1 and earlier allows remote authenticated users to execute arbitrary code as the root user via shell metacharacters in the cache_id parameter.

CVE-2016-8593

- log_query_system.cgi in Trend Micro Threat Discovery Appliance 2.6.1062r1 and earlier allows remote authenticated users to execute arbitrary code as the root user via shell metacharacters in the cache_id parameter.

CVE-2016-9651

- ** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.

CVE-2016-9793

- The sock_setsockopt function in net/core/sock.c in the Linux kernel before 4.8.14 mishandles negative values of sk_sndbuf and sk_rcvbuf, which allows local users to cause a denial of service (memory corruption and system crash) or possibly have unspecified other impact by leveraging the CAP_NET_ADMIN capability for a crafted setsockopt system call with the (1) SO_SNDBUFFORCE or (2) SO_RCVBUFFORCE option.

CVE-2016-10033

- The mailSend function in the isMail transport in PHPMailer before 5.2.18 might allow remote attackers to pass extra parameters to the mail command and consequently execute arbitrary code via a " (backslash double quote) in a crafted Sender property.

CVE-2016-10191

- Heap-based buffer overflow in libavformat/rtmppkt.c in FFmpeg before 2.8.10, 3.0.x before 3.0.5, 3.1.x before 3.1.6, and 3.2.x before 3.2.2 allows remote attackers to execute arbitrary code by leveraging failure to check for RTMP packet size mismatches.

CVE-2016-10277

- An elevation of privilege vulnerability in the Motorola bootloader could enable a local malicious application to execute arbitrary code within the context of the bootloader. This issue is rated as Critical due to the possibility of a local permanent device compromise, which may require reflashing the operating system to repair the device. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A-33840490.

CVE-2016-10370

- An issue was discovered on OnePlus devices such as the 3T. The OnePlus OTA Updater pushes the signed-OTA image over HTTP without TLS. While it does not allow for installation of arbitrary OTAs (due to the digital signature), it unnecessarily increases the attack surface, and allows for remote exploitation of other vulnerabilities such as CVE-2017-5948, CVE-2017-8850, and CVE-2017-8851.

CVE-2017-0015

- A remote code execution vulnerability exists in the way affected Microsoft scripting engines render when handling objects in memory in Microsoft browsers. These vulnerabilities could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability

could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. This vulnerability is different from those described in CVE-2017-0010, CVE-2017-0032, CVE-2017-0035, CVE-2017-0067, CVE-2017-0070, CVE-2017-0071, CVE-2017-0094, CVE-2017-0131, CVE-2017-0132, CVE-2017-0133, CVE-2017-0134, CVE-2017-0136, CVE-2017-0137, CVE-2017-0138, CVE-2017-0141, CVE-2017-0150, and CVE-2017-0151.

CVE-2017-0037

- Microsoft Internet Explorer 10 and 11 and Microsoft Edge have a type confusion issue in the `Layout::MultiColumnBoxBuilder::HandleColumnBreakOnColumnSpanningElement` function in `mshtml.dll`, which allows remote attackers to execute arbitrary code via vectors involving a crafted Cascading Style Sheets (CSS) token sequence and crafted JavaScript code that operates on a TH element.

CVE-2017-0059

- Microsoft Internet Explorer 9 through 11 allow remote attackers to obtain sensitive information from process memory via a crafted web site, aka "Internet Explorer Information Disclosure Vulnerability." This vulnerability is different from those described in CVE-2017-0008 and CVE-2017-0009.

CVE-2017-0070

- A remote code execution vulnerability exists in the way affected Microsoft scripting engines render when handling objects in memory in Microsoft browsers. These vulnerabilities could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. This vulnerability is different from those described in CVE-2017-0010, CVE-2017-0015, CVE-2017-0032, CVE-2017-0035, CVE-2017-0067, CVE-

2017-0071, CVE-2017-0094, CVE-2017-0131, CVE-2017-0132, CVE-2017-0133, CVE-2017-0134, CVE-2017-0136, CVE-2017-0137, CVE-2017-0138, CVE-2017-0141, CVE-2017-0150, and CVE-2017-0151.

CVE-2017-0071

- A remote code execution vulnerability exists in the way affected Microsoft scripting engines render when handling objects in memory in Microsoft browsers. These vulnerabilities could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. This vulnerability is different from those described in CVE-2017-0010, CVE-2017-0015, CVE-2017-0032, CVE-2017-0035, CVE-2017-0067, CVE-2017-0070, CVE-2017-0094, CVE-2017-0131, CVE-2017-0132, CVE-2017-0133, CVE-2017-0134, CVE-2017-0136, CVE-2017-0137, CVE-2017-0138, CVE-2017-0141, CVE-2017-0150, and CVE-2017-0151.

CVE-2017-0134

- A remote code execution vulnerability exists in the way affected Microsoft scripting engines render when handling objects in memory in Microsoft browsers. These vulnerabilities could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. This vulnerability is different from those described in CVE-2017-0010, CVE-2017-0015, CVE-2017-0032, CVE-2017-0035, CVE-2017-0067, CVE-2017-0070, CVE-2017-0071, CVE-2017-0094, CVE-2017-0131, CVE-2017-0132, CVE-2017-0133, CVE-2017-0136, CVE-2017-0137, CVE-2017-0138, CVE-2017-0141, CVE-2017-0150, and CVE-2017-0151.

CVE-2017-0141

- A remote code execution vulnerability exists in the way affected Microsoft scripting engines render when handling objects in memory in Microsoft browsers. These vulnerabilities could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. This vulnerability is different from those described in CVE-2017-0010, CVE-2017-0015, CVE-2017-0032, CVE-2017-0035, CVE-2017-0067, CVE-2017-0070, CVE-2017-0071, CVE-2017-0094, CVE-2017-0131, CVE-2017-0132, CVE-2017-0133, CVE-2017-0134, CVE-2017-0136, CVE-2017-0137, CVE-2017-0138, CVE-2017-0150, and CVE-2017-0151.

CVE-2017-0143

- The SMBv1 server in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT 8.1; and Windows 10 Gold, 1511, and 1607; and Windows Server 2016 allows remote attackers to execute arbitrary code via crafted packets, aka "Windows SMB Remote Code Execution Vulnerability." This vulnerability is different from those described in CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, and CVE-2017-0148.

CVE-2017-0144

- The SMBv1 server in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT 8.1; and Windows 10 Gold, 1511, and 1607; and Windows Server 2016 allows remote attackers to execute arbitrary code via crafted packets, aka "Windows SMB Remote Code Execution Vulnerability." This vulnerability is different from those described in CVE-2017-0143, CVE-2017-0145, CVE-2017-0146, and CVE-2017-0148.

CVE-2017-0145

- The SMBv1 server in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT 8.1; and Windows 10 Gold, 1511, and 1607; and Windows Server 2016 allows remote attackers to execute arbitrary code via crafted packets, aka "Windows SMB Remote Code Execution Vulnerability." This vulnerability is different from those described in CVE-2017-0143, CVE-2017-0144, CVE-2017-0146, and CVE-2017-0148.

CVE-2017-0146

- The SMBv1 server in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT 8.1; and Windows 10 Gold, 1511, and 1607; and Windows Server 2016 allows remote attackers to execute arbitrary code via crafted packets, aka "Windows SMB Remote Code Execution Vulnerability." This vulnerability is different from those described in CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, and CVE-2017-0148.

CVE-2017-0147

- The SMBv1 server in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT 8.1; and Windows 10 Gold, 1511, and 1607; and Windows Server 2016 allows remote attackers to obtain sensitive information from process memory via a crafted packets, aka "Windows SMB Information Disclosure Vulnerability."

CVE-2017-0148

- The SMBv1 server in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT 8.1; and Windows 10 Gold, 1511, and 1607; and Windows Server 2016 allows remote attackers to execute arbitrary code via crafted packets, aka "Windows SMB Remote Code Execution Vulnerability." This vulnerability is different from those described in CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, and CVE-2017-0146.

CVE-2017-0199

- Microsoft Office 2007 SP3, Microsoft Office 2010 SP2, Microsoft Office 2013 SP1, Microsoft Office 2016, Microsoft Windows Vista SP2, Windows Server 2008 SP2, Windows 7 SP1, Windows 8.1 allow remote attackers to execute arbitrary code via a crafted document, aka "Microsoft Office/WordPad Remote Code Execution Vulnerability w/Windows API."

CVE-2017-0213

- Windows COM Aggregate Marshaler in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows an elevation privilege vulnerability when an attacker runs a specially crafted application, aka "Windows COM Elevation of Privilege Vulnerability". This CVE ID is unique from CVE-2017-0214.

CVE-2017-0263

- The kernel-mode drivers in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allow local users to gain privileges via a crafted application, aka "Win32k Elevation of Privilege Vulnerability."

CVE-2017-0283

- Uniscribe in Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, Windows Server 2016, Microsoft Office 2007 SP3, Microsoft Office 2010 SP2, Microsoft Office Word Viewer, Microsoft Lync 2013 SP1, Skype for Business 2016, Microsoft Silverlight 5 Developer Runtime when installed on Microsoft Windows, and Microsoft Silverlight 5 when installed on Microsoft Windows allows a remote code execution vulnerability due to the way it handles objects in memory, aka "Windows Uniscribe Remote Code Execution Vulnerability". This CVE ID is unique from CVE-2017-8528.

CVE-2017-0290

- NScript in mpengine in Microsoft Malware Protection Engine with Engine Version before 1.1.13704.0, as used in Windows Defender and other products, allows remote attackers to execute arbitrary code or cause a denial of service (type confusion and application crash) via crafted JavaScript code within any file scanned by this engine.

CVE-2017-0392

- A denial of service vulnerability in VBRISeeker.cpp in libstagefright in Mediaserver could enable a remote attacker to use a specially crafted file to cause a device hang or reboot. This issue is rated as High due to the possibility of remote denial of service. Product: Android. Versions: 4.4.4, 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1. Android ID: A-32577290.

CVE-2017-0475

- An elevation of privilege vulnerability in the recovery verifier could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as Critical due to the possibility of a local permanent device compromise, which may require reflashing the operating system to repair the device. Product: Android. Versions: 4.4.4, 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-31914369.

CVE-2017-0497

- A denial of service vulnerability in Mediaserver could enable an attacker to use a specially crafted file to cause a device hang or reboot. This issue is rated as Moderate because it requires an uncommon device configuration. Product: Android. Versions: 7.0, 7.1.1. Android ID: A-33300701.

CVE-2017-0521

- An elevation of privilege vulnerability in the Qualcomm camera driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising

a privileged process. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A-32919951. References: QC-CR#1097709.

CVE-2017-0531

- An information disclosure vulnerability in the Qualcomm Wi-Fi driver could enable a local malicious application to access data outside of its permission levels. This issue is rated as Moderate because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A-32877245. References: QC-CR#1087469.

CVE-2017-0541

- A remote code execution vulnerability in sonivox in Mediaserver could enable an attacker using a specially crafted file to cause memory corruption during media file and data processing. This issue is rated as Critical due to the possibility of remote code execution within the context of the Mediaserver process. Product: Android. Versions: 4.4.4, 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-34031018.

CVE-2017-0548

- A remote denial of service vulnerability in libskia could enable an attacker to use a specially crafted file to cause a device hang or reboot. This issue is rated as High severity due to the possibility of remote denial of service. Product: Android. Versions: 7.0, 7.1.1. Android ID: A-33251605.

CVE-2017-0576

- An elevation of privilege vulnerability in the Qualcomm crypto engine driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A-33544431. References: QC-CR#1103089.

CVE-2017-0678

- A remote code execution vulnerability in the Android media framework. Product: Android. Versions: 7.0, 7.1.1, 7.1.2. Android ID: A-36576151.

CVE-2017-0714

- A remote code execution vulnerability in the Android media framework (h263 decoder). Product: Android. Versions: 4.4.4, 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2. Android ID: A-36492637.

CVE-2017-0718

- A remote code execution vulnerability in the Android media framework (mpeg2 decoder). Product: Android. Versions: 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2. Android ID: A-37273547.

CVE-2017-0719

- A remote code execution vulnerability in the Android media framework (mpeg2 decoder). Product: Android. Versions: 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2. Android ID: A-37273673.

CVE-2017-0720

- A remote code execution vulnerability in the Android media framework (libhevc). Product: Android. Versions: 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2. Android ID: A-37430213.

CVE-2017-0722

- A remote code execution vulnerability in the Android media framework (h263 decoder). Product: Android. Versions: 4.4.4, 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2. Android ID: A-37660827.

CVE-2017-0745

- A remote code execution vulnerability in the Android media framework (avc decoder). Product: Android. Versions: 4.4.4, 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2. Android ID: A-37079296.

CVE-2017-0758

- A remote code execution vulnerability in the Android media framework (libhevc). Product: Android. Versions: 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2. Android ID: A-36492741.

CVE-2017-0760

- A remote code execution vulnerability in the Android media framework (libstagefright). Product: Android. Versions: 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2. Android ID: A-37237396.

CVE-2017-0761

- A remote code execution vulnerability in the Android media framework (libavc). Product: Android. Versions: 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2, 8.0. Android ID: A-38448381.

CVE-2017-0764

- A remote code execution vulnerability in the Android media framework (libvorbis). Product: Android. Versions: 4.4.4, 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2, 8.0. Android ID: A-62872015.

CVE-2017-0776

- A information disclosure vulnerability in the Android media framework (n/a). Product: Android. Versions: 7.0, 7.1.1, 7.1.2, 8.0. Android ID: A-38496660.

CVE-2017-0777

- A information disclosure vulnerability in the Android media framework (n/a). Product: Android. Versions: 7.0, 7.1.1, 7.1.2. Android ID: A-38342499.

CVE-2017-0778

- A information disclosure vulnerability in the Android media framework (n/a). Product: Android. Versions: 7.0, 7.1.1, 7.1.2. Android ID: A-62133227.

CVE-2017-0781

- A remote code execution vulnerability in the Android system (bluetooth). Product: Android. Versions: 4.4.4, 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2, 8.0. Android ID: A-63146105.

CVE-2017-0785

- A information disclosure vulnerability in the Android system (bluetooth). Product: Android. Versions: 4.4.4, 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2, 8.0. Android ID: A-63146698.

CVE-2017-0813

- A denial of service vulnerability in the Android media framework (libstagefright). Product: Android. Versions: 7.0, 7.1.1, 7.1.2. Android ID: A-36531046.

CVE-2017-0814

- An information disclosure vulnerability in the Android media framework (n/a). Product: Android. Versions: 7.0, 7.1.1, 7.1.2, 8.0. Android ID: A-62800140.

CVE-2017-0820

- A vulnerability in the Android media framework (n/a). Product: Android. Versions: 7.0, 7.1.1, 7.1.2, 8.0. Android ID: A-62187433.

CVE-2017-1082

- ** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.

CVE-2017-1083

- ** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.

CVE-2017-1084

- ** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.

CVE-2017-1085

- ** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.

CVE-2017-2363

- An issue was discovered in certain Apple products. iOS before 10.2.1 is affected. Safari before 10.0.3 is affected. tvOS before 10.1.1 is affected. watchOS before 3.1.3 is affected. The issue involves the "WebKit" component. It allows remote attackers to bypass the Same Origin Policy and obtain sensitive information via a crafted web site.

CVE-2017-2364

- An issue was discovered in certain Apple products. iOS before 10.2.1 is affected. Safari before 10.0.3 is affected. The issue involves the "WebKit" component. It allows remote attackers to bypass the Same Origin Policy and obtain sensitive information via a crafted web site.

CVE-2017-2365

- An issue was discovered in certain Apple products. iOS before 10.2.1 is affected. Safari before 10.0.3 is affected. tvOS before 10.1.1 is affected. The issue involves the "WebKit" component. It allows remote attackers to bypass the Same Origin Policy and obtain sensitive information via a crafted web site.

CVE-2017-2367

- An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. tvOS before 10.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to bypass the Same Origin Policy and obtain sensitive information via a crafted web site.

CVE-2017-2416

- An issue was discovered in certain Apple products. iOS before 10.3 is affected. macOS before 10.12.4 is affected. tvOS before 10.2 is affected. watchOS before 3.2 is affected. The issue involves the "ImageIO" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted image file.

CVE-2017-2419

- An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. The issue involves the "WebKit" component. It allows remote attackers to bypass a Content Security Policy protection mechanism

via unspecified vectors.

CVE-2017-2426

- An issue was discovered in certain Apple products. macOS before 10.12.4 is affected. The issue involves the "iBooks" component. It allows remote attackers to obtain sensitive information from local files via a file: URL in an iBooks file.

CVE-2017-2442

- An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. The issue involves the "WebKit JavaScript Bindings" component. It allows remote attackers to bypass the Same Origin Policy and obtain sensitive information via a crafted web site.

CVE-2017-2445

- An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. tvOS before 10.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to conduct Universal XSS (UXSS) attacks via crafted frame objects.

CVE-2017-2446

- An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. tvOS before 10.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code via a crafted web site that leverages the mishandling of strict mode functions.

CVE-2017-2447

- An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. tvOS before 10.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to obtain sensitive

information or cause a denial of service (memory corruption) via a crafted web site.

CVE-2017-2460

- An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. tvOS before 10.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.

CVE-2017-2464

- An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. tvOS before 10.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.

CVE-2017-2475

- An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. tvOS before 10.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to conduct Universal XSS (UXSS) attacks via crafted use of frames on a web site.

CVE-2017-2479

- An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. iCloud before 6.2 on Windows is affected. iTunes before 12.6 on Windows is affected. tvOS before 10.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to bypass the Same Origin Policy and obtain sensitive information via a crafted web site.

CVE-2017-2480

- An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. iCloud before 6.2 on Windows is affected. iTunes before 12.6 on Windows is affected. tvOS before 10.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to bypass the Same Origin Policy and obtain sensitive information via a crafted web site.

CVE-2017-2491

- Use after free vulnerability in the String.replace method JavaScriptCore in Apple Safari in iOS before 10.3 allows remote attackers to execute arbitrary code via a crafted web page, or a crafted file.

CVE-2017-2493

- An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. iCloud before 6.2 on Windows is affected. tvOS before 10.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to bypass the Same Origin Policy and obtain sensitive information via a crafted elements on a web site.

CVE-2017-2504

- An issue was discovered in certain Apple products. iOS before 10.3.2 is affected. Safari before 10.1.1 is affected. tvOS before 10.2.1 is affected. The issue involves the "WebKit" component. It allows remote attackers to conduct Universal XSS (UXSS) attacks via a crafted web site that improperly interacts with WebKit Editor commands.

CVE-2017-2508

- An issue was discovered in certain Apple products. iOS before 10.3.2 is affected. Safari before 10.1.1 is affected. The issue involves the "WebKit" component. It allows remote attackers to conduct Universal XSS (UXSS) attacks via a crafted web site that improperly interacts with container nodes.

CVE-2017-2510

- An issue was discovered in certain Apple products. iOS before 10.3.2 is affected. Safari before 10.1.1 is affected. The issue involves the "WebKit" component. It allows remote attackers to conduct Universal XSS (UXSS) attacks via a crafted web site that improperly interacts with pageshow events.

CVE-2017-2521

- An issue was discovered in certain Apple products. iOS before 10.3.2 is affected. Safari before 10.1.1 is affected. tvOS before 10.2.1 is affected. watchOS before 3.2.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.

CVE-2017-2528

- An issue was discovered in certain Apple products. iOS before 10.3.2 is affected. Safari before 10.1.1 is affected. The issue involves the "WebKit" component. It allows remote attackers to conduct Universal XSS (UXSS) attacks via a crafted web site that improperly interacts with cached frames.

CVE-2017-2531

- An issue was discovered in certain Apple products. iOS before 10.3.2 is affected. Safari before 10.1.1 is affected. tvOS before 10.2.1 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.

CVE-2017-2536

- An issue was discovered in certain Apple products. iOS before 10.3.2 is affected. Safari before 10.1.1 is affected. tvOS before 10.2.1 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.

CVE-2017-2540

- An issue was discovered in certain Apple products. macOS before 10.12.5 is affected. The issue involves the "WindowServer" component. It allows attackers to bypass intended memory-read restrictions via a crafted app.

CVE-2017-2541

- An issue was discovered in certain Apple products. macOS before 10.12.5 is affected. The issue involves the "WindowServer" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app.

CVE-2017-2547

- An issue was discovered in certain Apple products. iOS before 10.3.2 is affected. Safari before 10.1.1 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.

CVE-2017-2636

- Race condition in drivers/tty/n_hdlc.c in the Linux kernel through 4.10.1 allows local users to gain privileges or cause a denial of service (double free) by setting the HDLC line discipline.

CVE-2017-2641

- In Moodle 2.x and 3.x, SQL injection can occur via user preferences.

CVE-2017-3066

- Adobe ColdFusion 2016 Update 3 and earlier, ColdFusion 11 update 11 and earlier, ColdFusion 10 Update 22 and earlier have a Java deserialization vulnerability in the Apache BlazeDS library. Successful exploitation could lead to arbitrary

code execution.

CVE-2017-3506

- Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: Web Services). Supported versions that are affected are 10.3.6.0, 12.1.3.0, 12.2.1.0, 12.2.1.1 and 12.2.1.2. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle WebLogic Server accessible data as well as unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data. CVSS 3.0 Base Score 7.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N).

CVE-2017-3599

- Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Pluggable Auth). Supported versions that are affected are 5.6.35 and earlier and 5.7.17 and earlier. Easily "exploitable" vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H). NOTE: the previous information is from the April 2017 CPU. Oracle has not commented on third-party claims that this issue is an integer overflow in sql/auth/sql_authentication.cc which allows remote attackers to cause a denial of service via a crafted authentication packet.

CVE-2017-3629

- Vulnerability in the Solaris component of Oracle Sun Systems Products Suite (subcomponent: Kernel). Supported versions that are affected are 10 and 11. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Solaris executes to compromise Solaris. Successful attacks of this vulnerability can result in

takeover of Solaris. CVSS 3.0 Base Score 7.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).

CVE-2017-3630

- Vulnerability in the Solaris component of Oracle Sun Systems Products Suite (subcomponent: Kernel). Supported versions that are affected are 10 and 11. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Solaris executes to compromise Solaris. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Solaris accessible data as well as unauthorized read access to a subset of Solaris accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Solaris. CVSS 3.0 Base Score 5.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L).

CVE-2017-3631

- Vulnerability in the Solaris component of Oracle Sun Systems Products Suite (subcomponent: Kernel). The supported version that is affected is 11. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Solaris executes to compromise Solaris. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Solaris accessible data as well as unauthorized read access to a subset of Solaris accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Solaris. CVSS 3.0 Base Score 5.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L).

CVE-2017-3881

- A vulnerability in the Cisco Cluster Management Protocol (CMP) processing code in Cisco IOS and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a reload of an affected device or remotely execute code with elevated privileges. The Cluster Management Protocol utilizes Telnet internally as a signaling and command protocol between cluster members. The vulnerability is due to the combination of two factors: (1) the failure to restrict the

use of CMP-specific Telnet options only to internal, local communications between cluster members and instead accept and process such options over any Telnet connection to an affected device; and (2) the incorrect processing of malformed CMP-specific Telnet options. An attacker could exploit this vulnerability by sending malformed CMP-specific Telnet options while establishing a Telnet session with an affected Cisco device configured to accept Telnet connections. An exploit could allow an attacker to execute arbitrary code and obtain full control of the device or cause a reload of the affected device. This affects Catalyst switches, Embedded Service 2020 switches, Enhanced Layer 2 EtherSwitch Service Module, Enhanced Layer 2/3 EtherSwitch Service Module, Gigabit Ethernet Switch Module (CGESM) for HP, IE Industrial Ethernet switches, ME 4924-10GE switch, RF Gateway 10, and SM-X Layer 2/3 EtherSwitch Service Module. Cisco Bug IDs: CSCvd48893.

CVE-2017-4901

- The drag-and-drop (DnD) function in VMware Workstation 12.x before version 12.5.4 and Fusion 8.x before version 8.5.5 has an out-of-bounds memory access vulnerability. This may allow a guest to execute code on the operating system that runs Workstation or Fusion.

CVE-2017-4914

- VMware vSphere Data Protection (VDP) 6.1.x, 6.0.x, 5.8.x, and 5.5.x contains a deserialization issue. Exploitation of this issue may allow a remote attacker to execute commands on the appliance.

CVE-2017-4915

- VMware Workstation Pro/Player contains an insecure library loading vulnerability via ALSA sound driver configuration files. Successful exploitation of this issue may allow unprivileged host users to escalate their privileges to root in a Linux host machine.

CVE-2017-4918

- VMware Horizon View Client (2.x, 3.x and 4.x prior to 4.5.0) contains a command injection vulnerability in the service startup script. Successful exploitation of this issue may allow unprivileged users to escalate their privileges to root on the Mac OSX system where the client is installed.

CVE-2017-4933

- VMware ESXi (6.5 before ESXi650-201710401-BG), Workstation (12.x before 12.5.8), and Fusion (8.x before 8.5.9) contain a vulnerability that could allow an authenticated VNC session to cause a heap overflow via a specific set of VNC packets resulting in heap corruption. Successful exploitation of this issue could result in remote code execution in a virtual machine via the authenticated VNC session. Note: In order for exploitation to be possible in ESXi, VNC must be manually enabled in a virtual machine's .vmx configuration file. In addition, ESXi must be configured to allow VNC traffic through the built-in firewall.

CVE-2017-4946

- The VMware V4H and V4PA desktop agents (6.x before 6.5.1) contain a privilege escalation vulnerability. Successful exploitation of this issue could result in a low privileged windows user escalating their privileges to SYSTEM.

CVE-2017-4971

- An issue was discovered in Pivotal Spring Web Flow through 2.4.4. Applications that do not change the value of the MvcViewFactoryCreator useSpringBinding property which is disabled by default (i.e., set to 'false') can be vulnerable to malicious EL expressions in view states that process form submissions but do not have a sub-element to declare explicit data binding property mappings.

CVE-2017-5007

- Blink in Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, and 56.0.2924.87 for Android, incorrectly handled the sequence of events when closing a page, which allowed a remote attacker to inject arbitrary scripts or HTML

(UXSS) via a crafted HTML page.

CVE-2017-5030

- Incorrect handling of complex species in V8 in Google Chrome prior to 57.0.2987.98 for Linux, Windows, and Mac and 57.0.2987.108 for Android allowed a remote attacker to execute arbitrary code via a crafted HTML page.

CVE-2017-5033

- Blink in Google Chrome prior to 57.0.2987.98 for Mac, Windows, and Linux and 57.0.2987.108 for Android failed to correctly propagate CSP restrictions to local scheme pages, which allowed a remote attacker to bypass content security policy via a crafted HTML page.

CVE-2017-5040

- V8 in Google Chrome prior to 57.0.2987.98 for Mac, Windows, and Linux and 57.0.2987.108 for Android was missing a neutering check, which allowed a remote attacker to read values in memory via a crafted HTML page.

CVE-2017-5053

- An out-of-bounds read in V8 in Google Chrome prior to 57.0.2987.133 for Linux, Windows, and Mac, and 57.0.2987.132 for Android, allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page, related to `Array.prototype.indexOf`.

CVE-2017-5070

- Type confusion in V8 in Google Chrome prior to 59.0.3071.86 for Linux, Windows, and Mac, and 59.0.3071.92 for Android, allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.

CVE-2017-5071

- Insufficient validation of untrusted input in V8 in Google Chrome prior to 59.0.3071.86 for Linux, Windows and Mac, and 59.0.3071.92 for Android allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.

CVE-2017-5088

- Insufficient validation of untrusted input in V8 in Google Chrome prior to 59.0.3071.104 for Mac, Windows, and Linux, and 59.0.3071.117 for Android, allowed a remote attacker to perform out of bounds memory access via a crafted HTML page.

CVE-2017-5098

- A use after free in V8 in Google Chrome prior to 60.0.3112.78 for Mac, Windows, Linux, and Android allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.

CVE-2017-5115

- Type confusion in V8 in Google Chrome prior to 61.0.3163.79 for Windows allowed a remote attacker to potentially exploit object corruption via a crafted HTML page.

CVE-2017-5116

- Type confusion in V8 in Google Chrome prior to 61.0.3163.79 for Mac, Windows, and Linux, and 61.0.3163.81 for Android, allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.

CVE-2017-5121

- Inappropriate use of JIT optimisation in V8 in Google Chrome prior to 61.0.3163.100 for Linux, Windows, and Mac allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page, related to the escape

analysis phase.

CVE-2017-5122

- Inappropriate use of table size handling in V8 in Google Chrome prior to 61.0.3163.100 for Windows allowed a remote attacker to trigger out-of-bounds access via a crafted HTML page.

CVE-2017-5123

- **** RESERVED **** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.

CVE-2017-5124

- Incorrect application of sandboxing in Blink in Google Chrome prior to 62.0.3202.62 allowed a remote attacker to inject arbitrary scripts or HTML (UXSS) via a crafted MHTML page.

CVE-2017-5126

- A use after free in PDFium in Google Chrome prior to 62.0.3202.62 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.

CVE-2017-5127

- Use after free in PDFium in Google Chrome prior to 62.0.3202.62 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.

CVE-2017-5128

- Heap buffer overflow in Blink in Google Chrome prior to 62.0.3202.62 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page, related to WebGL.

CVE-2017-5129

- A use after free in WebAudio in Blink in Google Chrome prior to 62.0.3202.62 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.

CVE-2017-5133

- Off-by-one read/write on the heap in Blink in Google Chrome prior to 62.0.3202.62 allowed a remote attacker to corrupt memory and possibly leak information and potentially execute code via a crafted PDF file.

CVE-2017-5135

- Certain Technicolor devices have an SNMP access-control bypass, possibly involving an ISP customization in some cases. The Technicolor (formerly Cisco) DPC3928SL with firmware D3928SL-P15-13-A386-c3420r55105-160127a could be reached by any SNMP community string from the Internet; also, you can write in the MIB because it provides write properties, aka Stringbleed. NOTE: the string-bleed/StringBleed-CVE-2017-5135 GitHub repository is not a valid reference as of 2017-04-27; it contains Trojan horse code purported to exploit this vulnerability.

CVE-2017-5622

- With OxygenOS before 4.0.3, when a charger is connected to a powered-off OnePlus 3 or 3T device, the platform starts with addb enabled. Therefore, a malicious charger or a physical attacker can open up, without authorization, an ADB session with the device, in order to further exploit other vulnerabilities and/or exfiltrate sensitive information.

CVE-2017-5624

- An issue was discovered in OxygenOS before 4.0.3 for OnePlus 3 and 3T. The attacker can persistently make the (locked) bootloader start the platform with dm-verity disabled, by issuing the 'fastboot oem disable_dm_verity' command. Having dm-verity disabled, the kernel will not verify the system partition (and any other dm-verity protected partition), which may allow for persistent code execution and privilege escalation.

CVE-2017-5626

- OxygenOS before version 4.0.2, on OnePlus 3 and 3T, has two hidden fastboot oem commands (4F500301 and 4F500302) that allow the attacker to lock/unlock the bootloader, disregarding the 'OEM Unlocking' checkbox, without user confirmation and without a factory reset. This allows for persistent code execution with high privileges (kernel/root) with complete access to user data.

CVE-2017-5638

- The Jakarta Multipart parser in Apache Struts 2 2.3.x before 2.3.32 and 2.5.x before 2.5.10.1 mishandles file upload, which allows remote attackers to execute arbitrary commands via a #cmd= string in a crafted Content-Type HTTP header, as exploited in the wild in March 2017.

CVE-2017-5689

- An unprivileged network attacker could gain system privileges to provisioned Intel manageability SKUs: Intel Active Management Technology (AMT) and Intel Standard Manageability (ISM). An unprivileged local attacker could provision manageability features gaining unprivileged network or local system privileges on Intel manageability SKUs: Intel Active Management Technology (AMT), Intel Standard Manageability (ISM), and Intel Small Business Technology (SBT).

CVE-2017-5715

- Systems with microprocessors utilizing speculative execution and indirect branch prediction may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis.

CVE-2017-5753

- Systems with microprocessors utilizing speculative execution and branch prediction may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis.

CVE-2017-5754

- Systems with microprocessors utilizing speculative execution and indirect branch prediction may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis of the data cache.

CVE-2017-5891

- ASUS RT-AC* and RT-N* devices with firmware before 3.0.0.4.380.7378 have Login Page CSRF and Save Settings CSRF.

CVE-2017-5892

- ASUS RT-AC* and RT-N* devices with firmware before 3.0.0.4.380.7378 allow JSONP Information Disclosure such as a network map.

CVE-2017-5948

- An issue was discovered on OnePlus One, X, 2, 3, and 3T devices. OxygenOS and HydrogenOS are vulnerable to downgrade attacks. This is due to a lenient 'updater-script' in OTAs that does not check that the current version is lower than or equal to the given image's. Downgrades can occur even on locked bootloaders and without triggering a factory reset, allowing for exploitation of now-patched vulnerabilities with access to user data. This vulnerability can be exploited by a Man-in-the-Middle (MiTM) attacker targeting the update process. This is possible because the update transaction does not occur over TLS (CVE-2016-10370). In addition, a physical attacker can reboot the phone into recovery, and then use 'adb sideload' to push the OTA (on OnePlus 3/3T 'Secure Start-up' must be off).

CVE-2017-6008

- A kernel pool overflow in the driver hitmanpro37.sys in Sophos SurfRight HitmanPro before 3.7.20 Build 286 (included in the HitmanPro.Alert solution and Sophos Clean) allows local users to escalate privileges via a malformed IOCTL call.

CVE-2017-6074

- The dccp_rcv_state_process function in net/dccp/input.c in the Linux kernel through 4.9.11 mishandles DCCP_PKT_REQUEST packet data structures in the LISTEN state, which allows local users to obtain root privileges or cause a denial of service (double free) via an application that makes an IPV6_RECVPKTINFO setsockopt system call.

CVE-2017-6178

- The IofCallDriver function in USBPcap 1.1.0.0 allows local users to gain privileges via a crafted 0x00090028 IOCTL call, which triggers a NULL pointer dereference.

CVE-2017-6326

- The Symantec Messaging Gateway can encounter an issue of remote code execution, which describes a situation whereby an individual may obtain the ability to execute commands remotely on a target machine or in a target process.

CVE-2017-6327

- The Symantec Messaging Gateway before 10.6.3-267 can encounter an issue of remote code execution, which describes a situation whereby an individual may obtain the ability to execute commands remotely on a target machine or in a target process. In this type of occurrence, after gaining access to the system, the attacker may attempt to elevate their privileges.

CVE-2017-6736

- The Simple Network Management Protocol (SNMP) subsystem of Cisco IOS 12.0 through 12.4 and 15.0 through 15.6 and IOS XE 2.2 through 3.17 contains multiple vulnerabilities that could allow an authenticated, remote attacker to remotely execute code on an affected system or cause an affected system to reload. An attacker could exploit these vulnerabilities by sending a crafted SNMP packet to an affected system via IPv4 or IPv6. Only traffic directed to an affected system can be used to exploit these vulnerabilities. The vulnerabilities are due to a buffer overflow condition in the SNMP subsystem of the affected software. The vulnerabilities affect all versions of SNMP: Versions 1, 2c, and 3. To exploit these vulnerabilities via SNMP Version 2c or earlier, the attacker must know the SNMP read-only community string for the affected system. To exploit these vulnerabilities via SNMP Version 3, the attacker must have user credentials for the affected system. All devices that have enabled SNMP and have not explicitly excluded the affected MIBs or OIDs should be considered vulnerable. Cisco Bug IDs: CSCve57697.

CVE-2017-6980

- An issue was discovered in certain Apple products. iOS before 10.3.2 is affected. Safari before 10.1.1 is affected. tvOS before 10.2.1 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.

CVE-2017-6984

- An issue was discovered in certain Apple products. iOS before 10.3.2 is affected. Safari before 10.1.1 is affected. iTunes before 12.6.1 on Windows is affected. tvOS before 10.2.1 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.

CVE-2017-7037

- An issue was discovered in certain Apple products. iOS before 10.3.3 is affected. Safari before 10.1.2 is affected. iCloud before 6.2.2 on Windows is affected. iTunes before 12.6.2 on Windows is affected. tvOS before 10.2.2 is affected. The

issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.

CVE-2017-7056

- An issue was discovered in certain Apple products. iOS before 10.3.3 is affected. Safari before 10.1.2 is affected. iCloud before 6.2.2 on Windows is affected. iTunes before 12.6.2 on Windows is affected. tvOS before 10.2.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.

CVE-2017-7061

- An issue was discovered in certain Apple products. iOS before 10.3.3 is affected. Safari before 10.1.2 is affected. iCloud before 6.2.2 on Windows is affected. iTunes before 12.6.2 on Windows is affected. tvOS before 10.2.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.

CVE-2017-7089

- An issue was discovered in certain Apple products. iOS before 11 is affected. Safari before 11 is affected. iCloud before 7.0 on Windows is affected. The issue involves the "WebKit" component. It allows remote attackers to conduct Universal XSS (UXSS) attacks via a crafted web site that is mishandled during parent-tab processing.

CVE-2017-7092

- An issue was discovered in certain Apple products. iOS before 11 is affected. Safari before 11 is affected. iCloud before 7.0 on Windows is affected. iTunes before 12.7 on Windows is affected. tvOS before 11 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.

CVE-2017-7115

- An issue was discovered in certain Apple products. iOS before 11 is affected. tvOS before 11 is affected. The issue involves the "Wi-Fi" component. It might allow remote attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via crafted Wi-Fi traffic that leverages a race condition.

CVE-2017-7117

- An issue was discovered in certain Apple products. iOS before 11 is affected. Safari before 11 is affected. iCloud before 7.0 on Windows is affected. iTunes before 12.7 on Windows is affected. tvOS before 11 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.

CVE-2017-7219

- A heap overflow vulnerability in Citrix NetScaler Gateway versions 10.1 before 135.8/135.12, 10.5 before 65.11, 11.0 before 70.12, and 11.1 before 52.13 allows a remote authenticated attacker to run arbitrary commands via unspecified vectors.

CVE-2017-7269

- Buffer overflow in the ScStoragePathFromUrl function in the WebDAV service in Internet Information Services (IIS) 6.0 in Microsoft Windows Server 2003 R2 allows remote attackers to execute arbitrary code via a long header beginning with "If: <http://" in a PROPFIND request, as exploited in the wild in July or August 2016.

CVE-2017-7279

- An unprivileged user of the Unitrends Enterprise Backup before 9.0.0 web server can escalate to root privileges by modifying the "token" cookie issued at login.

CVE-2017-7280

- An issue was discovered in `api/includes/systems.php` in Unitrends Enterprise Backup before 9.0.0. User input is not properly filtered before being sent to a `popen` function. This allows for remote code execution by sending a specially crafted user variable.

CVE-2017-7281

- An issue was discovered in Unitrends Enterprise Backup before 9.1.2. A lack of sanitization of user input in the `createReportName` and `saveReport` functions in `recoveryconsole/bpl/reports.php` allows for an authenticated user to create a randomly named file on disk with a user-controlled extension, contents, and path, leading to remote code execution, aka Unrestricted File Upload.

CVE-2017-7282

- An issue was discovered in Unitrends Enterprise Backup before 9.1.1. The function `downloadFile` in `api/includes/restore.php` blindly accepts any filename passed to `/api/restore/download` as valid. This allows an authenticated attacker to read any file in the filesystem that the web server has access to, aka Local File Inclusion (LFI).

CVE-2017-7283

- An authenticated user of Unitrends Enterprise Backup before 9.1.2 can execute arbitrary OS commands by sending a specially crafted filename to the `/api/restore/download-files` endpoint, related to the `downloadFiles` function in `api/includes/restore.php`.

CVE-2017-7293

- The DAX2API service installed as part of the Realtek Audio Driver on Windows 10 is vulnerable to a privilege escalation vulnerability which allows a normal user to get arbitrary system privileges.

CVE-2017-7308

- The `packet_set_ring` function in `net/packet/af_packet.c` in the Linux kernel through 4.10.6 does not properly validate certain block-size data, which allows local users to cause a denial of service (integer signedness error and out-of-bounds write), or gain privileges (if the `CAP_NET_RAW` capability is held), via crafted system calls.

CVE-2017-7344

- A privilege escalation in Fortinet FortiClient Windows 5.4.3 and earlier as well as 5.6.0 allows attacker to gain privilege via exploiting the Windows "security alert" dialog thereby popping up when the "VPN before logon" feature is enabled and an untrusted certificate chain.

CVE-2017-7442

- Nitro Pro 11.0.3.173 allows remote attackers to execute arbitrary code via `saveAs` and `launchURL` calls with directory traversal sequences.

CVE-2017-7494

- Samba since version 3.5.0 is vulnerable to remote code execution vulnerability, allowing a malicious client to upload a shared library to a writable share, and then cause the server to load and execute it.

CVE-2017-7504

- `HTTPServerILServlet.java` in JMS over HTTP Invocation Layer of the JbossMQ implementation, which is enabled by default in Red Hat Jboss Application Server <= Jboss 4.X does not restrict the classes for which it performs deserialization, which allows remote attackers to execute arbitrary code via crafted serialized data.

CVE-2017-7525

- A deserialization flaw was discovered in the jackson-databind, versions before 2.6.7.1, 2.7.9.1 and 2.8.9, which could allow an unauthenticated user to perform code execution by sending the maliciously crafted input to the readValue method of the ObjectMapper.

CVE-2017-7529

- Nginx versions since 0.5.6 up to and including 1.13.2 are vulnerable to integer overflow vulnerability in nginx range filter module resulting into leak of potentially sensitive information triggered by specially crafted request.

CVE-2017-7533

- Race condition in the fsnotify implementation in the Linux kernel through 4.12.4 allows local users to gain privileges or cause a denial of service (memory corruption) via a crafted application that leverages simultaneous execution of the inotify_handle_event and vfs_rename functions.

CVE-2017-8046

- Malicious PATCH requests submitted to spring-data-rest servers in Pivotal Spring Data REST versions prior to 2.5.12, 2.6.7, 3.0 RC3, Spring Boot versions prior to 2.0.0M4, and Spring Data release trains prior to Kay-RC3 can use specially crafted JSON data to run arbitrary Java code.

CVE-2017-8295

- WordPress through 4.7.4 relies on the Host HTTP header for a password-reset e-mail message, which makes it easier for remote attackers to reset arbitrary passwords by making a crafted wp-login.php?action=lostpassword request and then arranging for this message to bounce or be resent, leading to transmission of the reset key to a mailbox on an attacker-controlled SMTP server. This is related to problematic use of the SERVER_NAME variable in wp-includes/pluggable.php in conjunction with the PHP mail function. Exploitation is not achievable in all cases because it requires at least one of the following: (1) the attacker can prevent the victim from receiving any e-mail messages for an

extended period of time (such as 5 days), (2) the victim's e-mail system sends an autoresponse containing the original message, or (3) the victim manually composes a reply containing the original message.

CVE-2017-8386

- git-shell in git before 2.4.12, 2.5.x before 2.5.6, 2.6.x before 2.6.7, 2.7.x before 2.7.5, 2.8.x before 2.8.5, 2.9.x before 2.9.4, 2.10.x before 2.10.3, 2.11.x before 2.11.2, and 2.12.x before 2.12.3 might allow remote authenticated users to gain privileges via a repository name that starts with a - (dash) character.

CVE-2017-8464

- Windows Shell in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows local users or remote attackers to execute arbitrary code via a crafted .LNK file, which is not properly handled during icon display in Windows Explorer or any other application that parses the icon of the shortcut. aka "LNK Remote Code Execution Vulnerability."

CVE-2017-8514

- An information disclosure vulnerability exists when Microsoft SharePoint software fails to properly sanitize a specially crafted requests, aka "Microsoft SharePoint Reflective XSS Vulnerability".

CVE-2017-8543

- Microsoft Windows XP SP3, Windows XP x64 XP2, Windows Server 2003 SP2, Windows Vista, Windows 7 SP1, Windows Server 2008 SP2 and R2 SP1, Windows 8, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allow an attacker to take control of the affected system when Windows Search fails to handle objects in memory, aka "Windows Search Remote Code Execution Vulnerability".

CVE-2017-8548

- Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows an attacker to obtain information to further compromise the user's system when Microsoft Edge improperly handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-8499, CVE-2017-8520, CVE-2017-8521, and CVE-2017-8549.

CVE-2017-8570

- Microsoft Office allows a remote code execution vulnerability due to the way that it handles objects in memory, aka "Microsoft Office Remote Code Execution Vulnerability". This CVE ID is unique from CVE-2017-0243.

CVE-2017-8601

- Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allow an attacker to execute arbitrary code in the context of the current user when the JavaScript engine fails to render when handling objects in memory in Microsoft Edge, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-8596, CVE-2017-8610, CVE-2017-8618, CVE-2017-8619, CVE-2017-8603, CVE-2017-8604, CVE-2017-8605, CVE-2017-8606, CVE-2017-8607, CVE-2017-8608, CVE-2017-8598 and CVE-2017-8609.

CVE-2017-8625

- Internet Explorer in Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an attacker to bypass Device Guard User Mode Code Integrity (UMCI) policies due to Internet Explorer failing to validate UMCI policies, aka "Internet Explorer Security Feature Bypass Vulnerability".

CVE-2017-8634

- Microsoft Edge in Microsoft Windows 10 1703 allows an attacker to execute arbitrary code in the context of the current user due to the way that Microsoft browser JavaScript engines render content when handling objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-8635, CVE-2017-8636, CVE-2017-8638, CVE-2017-8639, CVE-2017-8640, CVE-2017-8641, CVE-2017-8645, CVE-2017-8646, CVE-2017-8647, CVE-2017-8655, CVE-2017-8656, CVE-2017-8657, CVE-2017-8670, CVE-2017-8671, CVE-2017-8672, and CVE-2017-8674.

CVE-2017-8636

- Microsoft browsers in Microsoft Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allow an attacker to execute arbitrary code in the context of the current user due to the way that Microsoft browser JavaScript engines render content when handling objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-8634, CVE-2017-8635, CVE-2017-8638, CVE-2017-8639, CVE-2017-8640, CVE-2017-8641, CVE-2017-8645, CVE-2017-8646, CVE-2017-8647, CVE-2017-8655, CVE-2017-8656, CVE-2017-8657, CVE-2017-8670, CVE-2017-8671, CVE-2017-8672, and CVE-2017-8674.

CVE-2017-8640

- Microsoft Edge in Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user due to the way that Microsoft browser JavaScript engines render content when handling objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-8634, CVE-2017-8635, CVE-2017-8636, CVE-2017-8638, CVE-2017-8639, CVE-2017-8641, CVE-2017-8645, CVE-2017-8646, CVE-2017-8647, CVE-2017-8655, CVE-2017-8656, CVE-2017-8657, CVE-2017-8670, CVE-2017-8671, CVE-2017-8672, and CVE-2017-8674.

CVE-2017-8645

- Microsoft Edge in Windows 10 1511, 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user due to the way that Microsoft browser JavaScript engines render content when handling objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-8634, CVE-2017-8635, CVE-2017-8636, CVE-2017-8638, CVE-2017-8639, CVE-2017-8640, CVE-2017-8641, CVE-2017-8646, CVE-2017-8647, CVE-2017-8655, CVE-2017-8656, CVE-2017-8657, CVE-2017-8670, CVE-2017-8671, CVE-2017-8672, and CVE-2017-8674.

CVE-2017-8646

- Microsoft Edge in Windows 10 1511, 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user due to the way that Microsoft browser JavaScript engines render content when handling objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-8634, CVE-2017-8635, CVE-2017-8636, CVE-2017-8638, CVE-2017-8639, CVE-2017-8640, CVE-2017-8641, CVE-2017-8645, CVE-2017-8647, CVE-2017-8655, CVE-2017-8656, CVE-2017-8657, CVE-2017-8670, CVE-2017-8671, CVE-2017-8672, and CVE-2017-8674.

CVE-2017-8656

- Microsoft Edge in Microsoft Windows 10 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user due to the way that Microsoft browser JavaScript engines render content when handling objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-8634, CVE-2017-8635, CVE-2017-8636, CVE-2017-8638, CVE-2017-8639, CVE-2017-8640, CVE-2017-8641, CVE-2017-8645, CVE-2017-8646, CVE-2017-8647, CVE-2017-8655, CVE-2017-8657, CVE-2017-8670, CVE-2017-8671, CVE-2017-8672, and CVE-2017-8674.

CVE-2017-8670

- Microsoft Edge in Microsoft Windows 10 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user due to the way that Microsoft browser JavaScript engines render content when

handling objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-8634, CVE-2017-8635, CVE-2017-8636, CVE-2017-8638, CVE-2017-8639, CVE-2017-8640, CVE-2017-8641, CVE-2017-8645, CVE-2017-8646, CVE-2017-8647, CVE-2017-8655, CVE-2017-8656, CVE-2017-8657, CVE-2017-8671, CVE-2017-8672, and CVE-2017-8674.

CVE-2017-8671

- Microsoft Edge in Microsoft Windows 10 1511, 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user due to the way that Microsoft browser JavaScript engines render content when handling objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-8634, CVE-2017-8635, CVE-2017-8636, CVE-2017-8638, CVE-2017-8639, CVE-2017-8640, CVE-2017-8641, CVE-2017-8645, CVE-2017-8646, CVE-2017-8647, CVE-2017-8655, CVE-2017-8656, CVE-2017-8657, CVE-2017-8670, CVE-2017-8672, and CVE-2017-8674.

CVE-2017-8729

- Microsoft Edge in Microsoft Windows 10 1703 allows an attacker to execute arbitrary code in the context of the current user, due to the way that the Microsoft Edge scripting engine handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-8649, CVE-2017-8660, CVE-2017-8738, CVE-2017-8740, CVE-2017-8741, CVE-2017-8748, CVE-2017-8752, CVE-2017-8753, CVE-2017-8755, CVE-2017-8756, and CVE-2017-11764.

CVE-2017-8740

- Microsoft Edge in Microsoft Windows 10 1703 allows an attacker to execute arbitrary code in the context of the current user, due to the way that the Microsoft Edge scripting engine handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-8649, CVE-2017-8660, CVE-2017-8729, CVE-2017-8738, CVE-2017-8740, CVE-2017-8741, CVE-2017-8748, CVE-2017-8752, CVE-2017-8753, CVE-2017-8755, CVE-2017-8756, and CVE-2017-11764.

CVE-2017-8751

- Microsoft Edge in Microsoft Windows 1703 allows an attacker to execute arbitrary code in the context of the current user, due to the way that Microsoft Edge accesses objects in memory, aka "Microsoft Edge Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-8731, CVE-2017-8734, and CVE-2017-11766.

CVE-2017-8755

- Microsoft Edge in Microsoft Windows 10 1511, 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to the way that the scripting engine handles objects in memory in Microsoft Edge, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-8649, CVE-2017-8649, CVE-2017-8660, CVE-2017-8729, CVE-2017-8738, CVE-2017-8740, CVE-2017-8741, CVE-2017-8748, CVE-2017-8752, CVE-2017-8753, CVE-2017-8756, and CVE-2017-11764.

CVE-2017-8759

- Microsoft .NET Framework 2.0, 3.5, 3.5.1, 4.5.2, 4.6, 4.6.1, 4.6.2 and 4.7 allow an attacker to execute code remotely via a malicious document or application, aka ".NET Framework Remote Code Execution Vulnerability."

CVE-2017-8817

- The FTP wildcard function in curl and libcurl before 7.57.0 allows remote attackers to cause a denial of service (out-of-bounds read and application crash) or possibly have unspecified other impact via a string that ends with an '[' character.

CVE-2017-8850

- An issue was discovered on OnePlus One, X, 2, 3, and 3T devices. Due to a lenient updater-script in the OnePlus OTA images, and the fact that both ROMs use the same OTA verification keys, attackers can install HydrogenOS over OxygenOS and vice versa, even on locked bootloaders, which allows for exploitation of vulnerabilities patched on one

image but not on the other, in addition to expansion of the attack surface. This vulnerability can be exploited by Man-in-the-Middle (MiTM) attackers targeting the update process. This is possible because the update transaction does not occur over TLS (CVE-2016-10370). In addition, physical attackers can reboot the phone into recovery, and then use 'adb sideload' to push the OTA (on OnePlus 3/3T 'Secure Start-up' must be off).

CVE-2017-8851

- An issue was discovered on OnePlus One and X devices. Due to a lenient updater-script on the OnePlus One and X OTA images, the fact that both products use the same OTA verification keys, and the fact that both products share the same 'ro.build.product' system property, attackers can install OTAs of one product over the other, even on locked bootloaders. That could theoretically allow for exploitation of vulnerabilities patched on one image but not on the other, in addition to expansion of the attack surface. Moreover, the vulnerability may result in having the device unusable until a Factory Reset is performed. This vulnerability can be exploited by Man-in-the-Middle (MiTM) attackers targeting the update process. This is possible because the update transaction does not occur over TLS (CVE-2016-10370). In addition, physical attackers can reboot the phone into recovery, and then use 'adb sideload' to push the OTA.

CVE-2017-8877

- ASUS RT-AC* and RT-N* devices with firmware through 3.0.0.4.380.7378 allow JSONP Information Disclosure such as the SSID.

CVE-2017-8878

- ASUS RT-AC* and RT-N* devices with firmware before 3.0.0.4.380.7378 allow remote authenticated users to discover the Wi-Fi password via WPS_info.xml.

CVE-2017-8890

- The `inet_csk_clone_lock` function in `net/ipv4/inet_connection_sock.c` in the Linux kernel through 4.10.15 allows attackers to cause a denial of service (double free) or possibly have unspecified other impact by leveraging use of the `accept` system call.

CVE-2017-8912

- **** DISPUTED **** CMS Made Simple (CMSMS) 2.1.6 allows remote authenticated administrators to execute arbitrary PHP code via the `code` parameter to `admin/editusertag.php`, related to the `CreateTagFunction` and `CallUserTag` functions.
NOTE: the vendor reportedly has stated this is "a feature, not a bug."

CVE-2017-8917

- SQL injection vulnerability in Joomla! 3.7.x before 3.7.1 allows attackers to execute arbitrary SQL commands via unspecified vectors.

CVE-2017-9417

- Broadcom BCM43xx Wi-Fi chips allow remote attackers to execute arbitrary code via unspecified vectors, aka the "Broadpwn" issue.

CVE-2017-9791

- The Struts 1 plugin in Apache Struts 2.3.x might allow remote code execution via a malicious field value passed in a raw message to the `ActionMessage`.

CVE-2017-9798

- Apache `httpd` allows remote attackers to read secret data from process memory if the `Limit` directive can be set in a user's `.htaccess` file, or if `httpd.conf` has certain misconfigurations, aka `Optionsbleed`. This affects the Apache HTTP

Server through 2.2.34 and 2.4.x through 2.4.27. The attacker sends an unauthenticated OPTIONS HTTP request when attempting to read secret data. This is a use-after-free issue and thus secret data is not always sent, and the specific data depends on many factors including configuration. Exploitation with .htaccess can be blocked with a patch to the `ap_limit_section` function in `server/core.c`.

CVE-2017-9805

- The REST Plugin in Apache Struts 2.1.2 through 2.3.x before 2.3.34 and 2.5.x before 2.5.13 uses an XStreamHandler with an instance of XStream for deserialization without any type filtering, which can lead to Remote Code Execution when deserializing XML payloads.

CVE-2017-9822

- DNN (aka DotNetNuke) before 9.1.1 has Remote Code Execution via a cookie, aka "2017-08 (Critical) Possible remote code execution on DNN sites."

CVE-2017-9948

- A stack buffer overflow vulnerability has been discovered in Microsoft Skype 7.2, 7.35, and 7.36 before 7.37, involving MSFTEDIT.DLL mishandling of remote RDP clipboard content within the message box.

CVE-2017-9993

- FFmpeg before 2.8.12, 3.0.x and 3.1.x before 3.1.9, 3.2.x before 3.2.6, and 3.3.x before 3.3.2 does not properly restrict HTTP Live Streaming filename extensions and demuxer names, which allows attackers to read arbitrary files via crafted playlist data.

CVE-2017-10271

- Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: WLS Security). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 12.2.1.1.0 and 12.2.1.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.0 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).

CVE-2017-10661

- Race condition in fs/timerfd.c in the Linux kernel before 4.10.15 allows local users to gain privileges or cause a denial of service (list corruption or use-after-free) via simultaneous file-descriptor operations that leverage improper might_cancel queueing.

CVE-2017-11105

- The OnePlus 2 Primary Bootloader (PBL) does not validate the SBL1 partition before executing it, although it contains a certificate. This allows attackers with write access to that partition to disable signature validation.

CVE-2017-11120

- On Broadcom BCM4355C0 Wi-Fi chips 9.44.78.27.0.1.56 and other chips, an attacker can craft a malformed RRM neighbor report frame to trigger an internal buffer overflow in the Wi-Fi firmware, aka B-V2017061204.

CVE-2017-11421

- gnome-exe-thumbnailer before 0.9.5 is prone to a VBScript Injection when generating thumbnails for MSI files, aka the "Bad Taste" issue. There is a local attack if the victim uses the GNOME Files file manager, and navigates to a directory containing a .msi file with VBScript code in its filename.

CVE-2017-11444

- Subrion CMS before 4.1.5.10 has a SQL injection vulnerability in /front/search.php via the \$_GET array.

CVE-2017-11610

- The XML-RPC server in supervisor before 3.0.1, 3.1.x before 3.1.4, 3.2.x before 3.2.4, and 3.3.x before 3.3.3 allows remote authenticated users to execute arbitrary commands via a crafted XML-RPC request, related to nested supervisord namespace lookups.

CVE-2017-11764

- Microsoft Edge in Microsoft Windows 10 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to the way that the Microsoft Edge scripting engine handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-8649, CVE-2017-8660, CVE-2017-8729, CVE-2017-8738, CVE-2017-8740, CVE-2017-8741, CVE-2017-8748, CVE-2017-8752, CVE-2017-8753, CVE-2017-8755, and CVE-2017-8756.

CVE-2017-11774

- Microsoft Outlook 2010 SP2, Outlook 2013 SP1 and RT SP1, and Outlook 2016 allow an attacker to execute arbitrary commands, due to how Microsoft Office handles objects in memory, aka "Microsoft Outlook Security Feature Bypass Vulnerability."

CVE-2017-11779

- The Microsoft Windows Domain Name System (DNS) DNSAPI.dll on Microsoft Windows 8.1, Windows Server 2012 R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows a remote code execution vulnerability when it fails to properly handle DNS responses, aka "Windows DNSAPI Remote Code Execution Vulnerability".

CVE-2017-11793

- Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 SP2 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-11792, CVE-2017-11796, CVE-2017-11798, CVE-2017-11799, CVE-2017-11800, CVE-2017-11801, CVE-2017-11802, CVE-2017-11804, CVE-2017-11805, CVE-2017-11806, CVE-2017-11807, CVE-2017-11808, CVE-2017-11809, CVE-2017-11810, CVE-2017-11811, CVE-2017-11812, and CVE-2017-11821.

CVE-2017-11799

- ChakraCore and Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-11792, CVE-2017-11793, CVE-2017-11796, CVE-2017-11797, CVE-2017-11798, CVE-2017-11800, CVE-2017-11801, CVE-2017-11802, CVE-2017-11804, CVE-2017-11805, CVE-2017-11806, CVE-2017-11807, CVE-2017-11808, CVE-2017-11809, CVE-2017-11810, CVE-2017-11811, CVE-2017-11812, and CVE-2017-11821.

CVE-2017-11802

- ChakraCore and Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-11792, CVE-2017-11793, CVE-2017-11796, CVE-2017-11797, CVE-2017-11798, CVE-2017-11799, CVE-2017-11800, CVE-2017-11801, CVE-2017-11804, CVE-2017-11805, CVE-2017-11806, CVE-2017-11807, CVE-2017-11808, CVE-2017-11809, CVE-2017-11810, CVE-2017-11811, CVE-2017-11812, and CVE-2017-11821.

CVE-2017-11809

- ChakraCore and Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-11792, CVE-2017-11793, CVE-2017-11796, CVE-2017-11797, CVE-2017-11798, CVE-2017-11799, CVE-2017-11800, CVE-2017-11801, CVE-2017-11802, CVE-2017-11804, CVE-2017-11805, CVE-2017-11806, CVE-2017-11807, CVE-2017-11808, CVE-2017-11810, CVE-2017-11811, CVE-2017-11812, and CVE-2017-11821.

CVE-2017-11811

- ChakraCore and Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-11792, CVE-2017-11793, CVE-2017-11796, CVE-2017-11797, CVE-2017-11798, CVE-2017-11799, CVE-2017-11800, CVE-2017-11801, CVE-2017-11802, CVE-2017-11804, CVE-2017-11805, CVE-2017-11806, CVE-2017-11807, CVE-2017-11808, CVE-2017-11809, CVE-2017-11810, CVE-2017-11812, and CVE-2017-11821.

CVE-2017-11812

- ChakraCore and Microsoft Edge in Microsoft Windows 10 1511, 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-11792, CVE-2017-11793, CVE-2017-11796, CVE-2017-11797, CVE-2017-11798, CVE-2017-11799, CVE-2017-11800, CVE-2017-11801, CVE-2017-11802, CVE-2017-11804, CVE-2017-11805, CVE-2017-11806, CVE-2017-11807, CVE-2017-11808, CVE-2017-11809, CVE-2017-11810, CVE-2017-11812, and CVE-2017-11821.

CVE-2017-11839

- Microsoft Edge in Windows 10 Gold, 1511, 1607, 1703, 1709, Windows Server 2016 and Windows Server, version 1709 allows an attacker to take control of an affected system, due to how the scripting engine handles objects in memory, aka

"Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-11836, CVE-2017-11837, CVE-2017-11838, CVE-2017-11840, CVE-2017-11841, CVE-2017-11843, CVE-2017-11846, CVE-2017-11858, CVE-2017-11859, CVE-2017-11861, CVE-2017-11862, CVE-2017-11866, CVE-2017-11869, CVE-2017-11870, CVE-2017-11871, and CVE-2017-11873.

CVE-2017-11840

- ChakraCore and Microsoft Edge in Windows 10 Gold, 1511, 1607, 1703, 1709, Windows Server 2016 and Windows Server, version 1709 allows an attacker to gain the same user rights as the current user, due to how the scripting engine handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-11836, CVE-2017-11837, CVE-2017-11838, CVE-2017-11839, CVE-2017-11841, CVE-2017-11843, CVE-2017-11846, CVE-2017-11858, CVE-2017-11859, CVE-2017-11861, CVE-2017-11862, CVE-2017-11866, CVE-2017-11869, CVE-2017-11870, CVE-2017-11871, and CVE-2017-11873.

CVE-2017-11841

- ChakraCore and Microsoft Edge in Windows 10 Gold, 1511, 1607, 1703, 1709, Windows Server 2016 and Windows Server, version 1709 allows an attacker to gain the same user rights as the current user, due to how the scripting engine handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-11836, CVE-2017-11837, CVE-2017-11838, CVE-2017-11839, CVE-2017-11840, CVE-2017-11843, CVE-2017-11846, CVE-2017-11858, CVE-2017-11859, CVE-2017-11861, CVE-2017-11862, CVE-2017-11866, CVE-2017-11869, CVE-2017-11870, CVE-2017-11871, and CVE-2017-11873.

CVE-2017-11855

- Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 SP2 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, 1709, Windows Server 2016 and Windows Server, version 1709 allows an attacker to gain the same user rights as the current user, due to how Internet Explorer

handles objects in memory, aka "Internet Explorer Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-11856.

CVE-2017-11861

- Microsoft Edge in Windows 10 1607, 1703, 1709, Windows Server 2016 and Windows Server, version 1709 allows an attacker to gain the same user rights as the current user, due to how the scripting engine handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-11836, CVE-2017-11837, CVE-2017-11838, CVE-2017-11839, CVE-2017-11840, CVE-2017-11841, CVE-2017-11843, CVE-2017-11846, CVE-2017-11858, CVE-2017-11859, CVE-2017-11862, CVE-2017-11866, CVE-2017-11869, CVE-2017-11870, CVE-2017-11871, and CVE-2017-11873.

CVE-2017-11870

- ChakraCore and Microsoft Edge in Windows 10 1703, 1709, and Windows Server, version 1709 allows an attacker to gain the same user rights as the current user, due to how the scripting engine handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-11836, CVE-2017-11837, CVE-2017-11838, CVE-2017-11839, CVE-2017-11840, CVE-2017-11841, CVE-2017-11843, CVE-2017-11846, CVE-2017-11858, CVE-2017-11859, CVE-2017-11861, CVE-2017-11862, CVE-2017-11866, CVE-2017-11869, CVE-2017-11871, and CVE-2017-11873.

CVE-2017-11873

- ChakraCore and Microsoft Edge in Windows 10 1511, 1607, 1703, 1709, Windows Server 2016 and Windows Server, version 1709 allows an attacker to gain the same user rights as the current user, due to how the scripting engine handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-11836, CVE-2017-11837, CVE-2017-11838, CVE-2017-11839, CVE-2017-11840, CVE-2017-11841, CVE-2017-11843, CVE-2017-11846, CVE-2017-11858, CVE-2017-11859, CVE-2017-11861, CVE-2017-11862, CVE-2017-11866, CVE-2017-11869, CVE-2017-11870, and CVE-2017-11871.

CVE-2017-11882

- Microsoft Office 2007 Service Pack 3, Microsoft Office 2010 Service Pack 2, Microsoft Office 2013 Service Pack 1, and Microsoft Office 2016 allow an attacker to run arbitrary code in the context of the current user by failing to properly handle objects in memory, aka "Microsoft Office Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-11884.

CVE-2017-11890

- Microsoft Windows 7 SP1, Windows Server 2008 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allow an attacker to execute arbitrary code in the context of the current user, due to how Internet Explorer handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-11886, CVE-2017-11889, CVE-2017-11893, CVE-2017-11894, CVE-2017-11895, CVE-2017-11901, CVE-2017-11903, CVE-2017-11905, CVE-2017-11907, CVE-2017-11908, CVE-2017-11909, CVE-2017-11910, CVE-2017-11911, CVE-2017-11912, CVE-2017-11913, CVE-2017-11914, CVE-2017-11916, CVE-2017-11918, and CVE-2017-11930.

CVE-2017-11893

- ChakraCore and Microsoft Edge in Windows 10 1511, 1607, 1703, 1709, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-11886, CVE-2017-11889, CVE-2017-11890, CVE-2017-11894, CVE-2017-11895, CVE-2017-11901, CVE-2017-11903, CVE-2017-11905, CVE-2017-11907, CVE-2017-11908, CVE-2017-11909, CVE-2017-11910, CVE-2017-11911, CVE-2017-11912, CVE-2017-11913, CVE-2017-11914, CVE-2017-11916, CVE-2017-11918, and CVE-2017-11930.

CVE-2017-11903

- Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows an attacker to gain the same user rights as the current user, due to how Internet Explorer handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-11886, CVE-2017-11889, CVE-2017-11890, CVE-2017-11893, CVE-2017-11894, CVE-2017-11895, CVE-2017-11901, CVE-2017-11905, CVE-2017-11907, CVE-2017-11908, CVE-2017-11909, CVE-2017-11910, CVE-2017-11911, CVE-2017-11912, CVE-2017-11913, CVE-2017-11914, CVE-2017-11916, CVE-2017-11918, and CVE-2017-11930.

CVE-2017-11906

- Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, and Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows an attacker to obtain information to further compromise the user's system, due to how Internet Explorer handles objects in memory, aka "Scripting Engine Information Disclosure Vulnerability". This CVE ID is unique from CVE-2017-11887 and CVE-2017-11919.

CVE-2017-11907

- Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows an attacker to gain the same user rights as the current user, due to how Internet Explorer handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-11886, CVE-2017-11889, CVE-2017-11890, CVE-2017-11893, CVE-2017-11894, CVE-2017-11895, CVE-2017-11901, CVE-2017-11903, CVE-2017-11905, CVE-2017-11905, CVE-2017-11908, CVE-2017-11909, CVE-2017-11910, CVE-2017-11911, CVE-2017-11912, CVE-2017-11913, CVE-2017-11914, CVE-2017-11916, CVE-2017-11918, and CVE-2017-11930.

CVE-2017-11909

- ChakraCore and Windows 10 1511, 1607, 1703, 1709, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-11886, CVE-2017-11889, CVE-2017-11890, CVE-2017-11893, CVE-2017-11894, CVE-2017-11895, CVE-2017-11901, CVE-2017-11903, CVE-2017-11905, CVE-2017-11905, CVE-2017-11907, CVE-2017-11908, CVE-2017-11910, CVE-2017-11911, CVE-2017-11912, CVE-2017-11913, CVE-2017-11914, CVE-2017-11916, CVE-2017-11918, and CVE-2017-11930.

CVE-2017-11911

- ChakraCore and Windows 10 1511, 1607, 1703, 1709, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-11886, CVE-2017-11889, CVE-2017-11890, CVE-2017-11893, CVE-2017-11894, CVE-2017-11895, CVE-2017-11901, CVE-2017-11903, CVE-2017-11905, CVE-2017-11905, CVE-2017-11907, CVE-2017-11908, CVE-2017-11909, CVE-2017-11910, CVE-2017-11912, CVE-2017-11913, CVE-2017-11914, CVE-2017-11916, CVE-2017-11918, and CVE-2017-11930.

CVE-2017-11914

- ChakraCore and Microsoft Edge in Windows 10 1511, 1607, 1703, 1709, and Windows Server 2016 allows an attacker to gain the same user rights as the current user, due to how the scripting engine handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-11886, CVE-2017-11889, CVE-2017-11890, CVE-2017-11893, CVE-2017-11894, CVE-2017-11895, CVE-2017-11901, CVE-2017-11903, CVE-2017-11905, CVE-2017-11905, CVE-2017-11907, CVE-2017-11908, CVE-2017-11909, CVE-2017-11910, CVE-2017-11911, CVE-2017-11912, CVE-2017-11913, CVE-2017-11916, CVE-2017-11918, and CVE-2017-11930.

CVE-2017-11918

- ChakraCore and Microsoft Edge in Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows an attacker to gain the same user rights as the current user, due to how the scripting engine handles objects in memory, aka

"Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-11886, CVE-2017-11889, CVE-2017-11890, CVE-2017-11893, CVE-2017-11894, CVE-2017-11895, CVE-2017-11901, CVE-2017-11903, CVE-2017-11905, CVE-2017-11905, CVE-2017-11907, CVE-2017-11908, CVE-2017-11909, CVE-2017-11910, CVE-2017-11911, CVE-2017-11912, CVE-2017-11913, CVE-2017-11914, CVE-2017-11916, and CVE-2017-11930.

CVE-2017-12097

- An exploitable cross site scripting (XSS) vulnerability exists in the filter functionality of the delayed_job_web rails gem version 1.4. A specially crafted URL can cause an XSS flaw resulting in an attacker being able to execute arbitrary javascript on the victim's browser. An attacker can phish an authenticated user to trigger this vulnerability.

CVE-2017-12098

- An exploitable cross site scripting (XSS) vulnerability exists in the add filter functionality of the rails_admin rails gem version 1.2.0. A specially crafted URL can cause an XSS flaw resulting in an attacker being able to execute arbitrary javascript on the victim's browser. An attacker can phish an authenticated user to trigger this vulnerability.

CVE-2017-12149

- In Jboss Application Server as shipped with Red Hat Enterprise Application Platform 5.2, it was found that the doFilter method in the ReadOnlyAccessFilter of the HTTP Invoker does not restrict classes for which it performs deserialization and thus allowing an attacker to execute arbitrary code via crafted serialized data.

CVE-2017-12542

- A authentication bypass and execution of code vulnerability in HPE Integrated Lights-out 4 (iLO 4) version prior to 2.53 was found.

CVE-2017-12581

- GitHub Electron before 1.6.8 allows remote command execution because of a nodeIntegration bypass vulnerability. This also affects all applications that bundle Electron code equivalent to 1.6.8 or earlier. Bypassing the Same Origin Policy (SOP) is a precondition; however, recent Electron versions do not have strict SOP enforcement. Combining an SOP bypass with a privileged URL internally used by Electron, it was possible to execute native Node.js primitives in order to run OS commands on the user's host. Specifically, a chrome-devtools://devtools/bundled/inspector.html window could be used to eval a Node.js `child_process.execFile` API call.

CVE-2017-12611

- In Apache Struts 2.0.1 through 2.3.33 and 2.5 through 2.5.10, using an unintentional expression in a Freemarker tag instead of string literals can lead to a RCE attack.

CVE-2017-12615

- When running Apache Tomcat 7.0.0 to 7.0.79 on Windows with HTTP PUTs enabled (e.g. via setting the `readonly` initialisation parameter of the `Default` to `false`) it was possible to upload a JSP file to the server via a specially crafted request. This JSP could then be requested and any code it contained would be executed by the server.

CVE-2017-12617

- When running Apache Tomcat versions 9.0.0.M1 to 9.0.0, 8.5.0 to 8.5.22, 8.0.0.RC1 to 8.0.46 and 7.0.0 to 7.0.81 with HTTP PUTs enabled (e.g. via setting the `readonly` initialisation parameter of the `Default` servlet to `false`) it was possible to upload a JSP file to the server via a specially crafted request. This JSP could then be requested and any code it contained would be executed by the server.

CVE-2017-13089

- The `http.c:skip_short_body()` function is called in some circumstances, such as when processing redirects. When the response is sent chunked in `wget` before 1.19.2, the chunk parser uses `strtol()` to read each chunk's length, but doesn't

check that the chunk length is a non-negative number. The code then tries to skip the chunk in pieces of 512 bytes by using the MIN() macro, but ends up passing the negative chunk length to connect.c:fd_read(). As fd_read() takes an int argument, the high 32 bits of the chunk length are discarded, leaving fd_read() with a completely attacker controlled length argument.

CVE-2017-13253

- In CryptoPlugin::decrypt of CryptoPlugin.cpp, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation. Product: Android. Versions: 8.0, 8.1. Android ID: A-71389378.

CVE-2017-13258

- In bnep_data_ind of bnep_main.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android. Versions: 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2, 8.0, 8.1. Android ID: A-67863755.

CVE-2017-13260

- In bnep_data_ind of bnep_main.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android. Versions: 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2, 8.0, 8.1. Android ID: A-69177251.

CVE-2017-13261

- In bnep_process_control_packet of bnep_utils.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android. Versions: 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2, 8.0, 8.1. Android ID: A-69177292.

CVE-2017-13262

- In `bnep_data_ind` of `bnep_main.cc`, there is a possible out of bounds read due to a missing length decrement operation. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android. Versions: 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2, 8.0, 8.1. Android ID: A-69271284.

CVE-2017-13791

- An issue was discovered in certain Apple products. iOS before 11.1 is affected. Safari before 11.0.1 is affected. iCloud before 7.1 on Windows is affected. iTunes before 12.7.1 on Windows is affected. tvOS before 11.1 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.

CVE-2017-13792

- An issue was discovered in certain Apple products. iOS before 11.1 is affected. Safari before 11.0.1 is affected. iCloud before 7.1 on Windows is affected. iTunes before 12.7.1 on Windows is affected. tvOS before 11.1 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.

CVE-2017-14335

- On Beijing Hanbang Hanbanggaoke devices, because user-controlled input is not sufficiently sanitized, sending a PUT request to `/ISAPI/Security/users/1` allows an admin password change.

CVE-2017-14491

- Heap-based buffer overflow in `dnsmasq` before 2.78 allows remote attackers to cause a denial of service (crash) or execute arbitrary code via a crafted DNS response.

CVE-2017-14492

- Heap-based buffer overflow in dnsmasq before 2.78 allows remote attackers to cause a denial of service (crash) or execute arbitrary code via a crafted IPv6 router advertisement request.

CVE-2017-14493

- Stack-based buffer overflow in dnsmasq before 2.78 allows remote attackers to cause a denial of service (crash) or execute arbitrary code via a crafted DHCPv6 request.

CVE-2017-14494

- dnsmasq before 2.78, when configured as a relay, allows remote attackers to obtain sensitive memory information via vectors involving handling DHCPv6 forwarded requests.

CVE-2017-14495

- Memory leak in dnsmasq before 2.78, when the --add-mac, --add-cpe-id or --add-subnet option is specified, allows remote attackers to cause a denial of service (memory consumption) via vectors involving DNS response creation.

CVE-2017-14496

- Integer underflow in the add_pseudoheader function in dnsmasq before 2.78 , when the --add-mac, --add-cpe-id or --add-subnet option is specified, allows remote attackers to cause a denial of service via a crafted DNS request.

CVE-2017-14904

- In Android for MSM, Firefox OS for MSM, QRD Android, with all Android releases from CAF using the Linux kernel, a crafted binder request can cause an arbitrary unmap in MediaServer.

CVE-2017-15303

- In CPUID CPU-Z before 1.43, there is an arbitrary memory write that results directly in elevation of privileges, because any program running on the local machine (while CPU-Z is running) can issue an ioctl 0x9C402430 call to the kernel-mode driver (e.g., cpuz141_x64.sys for version 1.41).

CVE-2017-15361

- The Infineon RSA library 1.02.013 in Infineon Trusted Platform Module (TPM) firmware, such as versions before 00000000000000422 - 4.34, before 0000000000000062b - 6.43, and before 000000000000008521 - 133.33, mishandles RSA key generation, which makes it easier for attackers to defeat various cryptographic protection mechanisms via targeted attacks, aka ROCA. Examples of affected technologies include BitLocker with TPM 1.2, YubiKey 4 (before 4.3.5) PGP key generation, and the Cached User Data encryption feature in Chrome OS.

CVE-2017-15388

- Iteration through non-finite points in Skia in Google Chrome prior to 62.0.3202.62 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.

CVE-2017-15396

- **** RESERVED **** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.

CVE-2017-15398

- **** RESERVED **** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.

CVE-2017-15399

- **** RESERVED **** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.

CVE-2017-15401

- **** RESERVED **** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.

CVE-2017-15411

- **** RESERVED **** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.

CVE-2017-15412

- **** RESERVED **** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.

CVE-2017-15415

- **** RESERVED **** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.

CVE-2017-15428

- **** RESERVED **** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.

CVE-2017-15613

- TP-Link WVR, WAR and ER devices allow remote authenticated administrators to execute arbitrary commands via command injection in the new-interface variable in the cmxddns.lua file.

CVE-2017-15614

- TP-Link WVR, WAR and ER devices allow remote authenticated administrators to execute arbitrary commands via command injection in the new-outif variable in the ptp_client.lua file.

CVE-2017-15615

- TP-Link WVR, WAR and ER devices allow remote authenticated administrators to execute arbitrary commands via command injection in the lcpechointerval variable in the ptp_client.lua file.

CVE-2017-15616

- TP-Link WVR, WAR and ER devices allow remote authenticated administrators to execute arbitrary commands via command injection in the new-interface variable in the phddns.lua file.

CVE-2017-15617

- TP-Link WVR, WAR and ER devices allow remote authenticated administrators to execute arbitrary commands via command injection in the iface variable in the interface_wan.lua file.

CVE-2017-15618

- TP-Link WVR, WAR and ER devices allow remote authenticated administrators to execute arbitrary commands via command injection in the new-enable variable in the ptp_client.lua file.

CVE-2017-15619

- TP-Link WVR, WAR and ER devices allow remote authenticated administrators to execute arbitrary commands via command injection in the ptphellointerval variable in the ptp_client.lua file.

CVE-2017-15620

- TP-Link WVR, WAR and ER devices allow remote authenticated administrators to execute arbitrary commands via command injection in the new-zone variable in the ipmac_import.lua file.

CVE-2017-15621

- TP-Link WVR, WAR and ER devices allow remote authenticated administrators to execute arbitrary commands via command injection in the olmode variable in the interface_wan.lua file.

CVE-2017-15622

- TP-Link WVR, WAR and ER devices allow remote authenticated administrators to execute arbitrary commands via command injection in the new-mppeencryption variable in the ptp_client.lua file.

CVE-2017-15623

- TP-Link WVR, WAR and ER devices allow remote authenticated administrators to execute arbitrary commands via command injection in the new-enable variable in the ptp_server.lua file.

CVE-2017-15624

- TP-Link WVR, WAR and ER devices allow remote authenticated administrators to execute arbitrary commands via command injection in the new-authype variable in the ptp_server.lua file.

CVE-2017-15625

- TP-Link WVR, WAR and ER devices allow remote authenticated administrators to execute arbitrary commands via command injection in the new-olmode variable in the ptp_client.lua file.

CVE-2017-15626

- TP-Link WVR, WAR and ER devices allow remote authenticated administrators to execute arbitrary commands via command injection in the new-bindif variable in the ptp_server.lua file.

CVE-2017-15627

- TP-Link WVR, WAR and ER devices allow remote authenticated administrators to execute arbitrary commands via command injection in the new-pns variable in the ptp_client.lua file.

CVE-2017-15628

- TP-Link WVR, WAR and ER devices allow remote authenticated administrators to execute arbitrary commands via command injection in the lcpchointerval variable in the ptp_server.lua file.

CVE-2017-15629

- TP-Link WVR, WAR and ER devices allow remote authenticated administrators to execute arbitrary commands via command injection in the new-tunnelname variable in the ptp_client.lua file.

CVE-2017-15630

- TP-Link WVR, WAR and ER devices allow remote authenticated administrators to execute arbitrary commands via command injection in the new-remotesubnet variable in the ptp_client.lua file.

CVE-2017-15631

- TP-Link WVR, WAR and ER devices allow remote authenticated administrators to execute arbitrary commands via command injection in the new-workmode variable in the ptp_client.lua file.

CVE-2017-15632

- TP-Link WVR, WAR and ER devices allow remote authenticated administrators to execute arbitrary commands via command injection in the new-mppeencryption variable in the ptp_server.lua file.

CVE-2017-15633

- TP-Link WVR, WAR and ER devices allow remote authenticated administrators to execute arbitrary commands via command injection in the new-ipgroup variable in the session_limits.lua file.

CVE-2017-15634

- TP-Link WVR, WAR and ER devices allow remote authenticated administrators to execute arbitrary commands via command injection in the name variable in the wportal.lua file.

CVE-2017-15635

- TP-Link WVR, WAR and ER devices allow remote authenticated administrators to execute arbitrary commands via command injection in the max_conn variable in the session_limits.lua file.

CVE-2017-15636

- TP-Link WVR, WAR and ER devices allow remote authenticated administrators to execute arbitrary commands via command injection in the new-time variable in the webfilter.lua file.

CVE-2017-15637

- TP-Link WVR, WAR and ER devices allow remote authenticated administrators to execute arbitrary commands via command injection in the ptphellointerval variable in the ptp_server.lua file.

CVE-2017-15944

- Palo Alto Networks PAN-OS before 6.1.19, 7.0.x before 7.0.19, 7.1.x before 7.1.14, and 8.0.x before 8.0.6 allows remote attackers to execute arbitrary code via vectors involving the management interface.

CVE-2017-16544

- In the add_match function in libbb/lineedit.c in BusyBox through 1.27.2, the tab autocomplete feature of the shell, used to get a list of filenames in a directory, does not sanitize filenames and results in executing any escape sequence in the terminal. This could potentially result in code execution, arbitrary file writes, or other attacks.

CVE-2017-16584

- This vulnerability allows remote attackers to disclose sensitive information on vulnerable installations of Foxit Reader 8.3.2.25013. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within util.printf. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated object. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-5290.

CVE-2017-16716

- A SQL Injection issue was discovered in WebAccess versions prior to 8.3. WebAccess does not properly sanitize its inputs for SQL commands.

CVE-2017-16943

- The receive_msg function in receive.c in the SMTP daemon in Exim 4.88 and 4.89 allows remote attackers to execute arbitrary code or cause a denial of service (use-after-free) via vectors involving BDAT commands.

CVE-2017-16944

- The receive_msg function in receive.c in the SMTP daemon in Exim 4.88 and 4.89 allows remote attackers to cause a denial of service (infinite loop and stack exhaustion) via vectors involving BDAT commands and an improper check for a '.' character signifying the end of the content, related to the bdat_getc function.

CVE-2017-16995

- The check_alu_op function in kernel/bpf/verifier.c in the Linux kernel through 4.14.8 allows local users to cause a denial of service (memory corruption) or possibly have unspecified other impact by leveraging incorrect sign extension.

CVE-2017-17033

- A buffer overflow vulnerability in password function in QNAP QTS version 4.2.6 build 20171026, 4.3.3.0378 build 20171117, 4.3.4.0387 (Beta 2) build 20171116 and earlier could allow remote attackers to execute arbitrary code on NAS devices.

CVE-2017-17107

- Zivif PR115-204-P-RS V2.3.4.2103 web cameras contain a hard-coded cat1029 password for the root user. The SONIX operating system's setup renders this password unchangeable and it can be used to access the device via a TELNET session.

CVE-2017-17215

- Huawei HG532 with some customized versions has a remote code execution vulnerability. An authenticated attacker could send malicious packets to port 37215 to launch attacks. Successful exploit could lead to the remote execution of arbitrary code.

CVE-2017-17405

- Ruby before 2.4.3 allows Net::FTP command injection. Net::FTP#get, getbinaryfile, gettextfile, put, putbinaryfile, and puttextfile use Kernel#open to open a local file. If the localfile argument starts with the "|" pipe character, the command following the pipe character is executed. The default value of localfile is File.basename(remotefile), so malicious FTP servers could cause arbitrary command execution.

CVE-2017-17562

- Embedthis GoAhead before 3.6.5 allows remote code execution if CGI is enabled and a CGI program is dynamically linked. This is a result of initializing the environment of forked CGI scripts using untrusted HTTP request parameters in the cgiHandler function in cgi.c. When combined with the glibc dynamic linker, this behaviour can be abused for remote code execution using special parameter names such as LD_PRELOAD. An attacker can POST their shared object payload in the body of the request, and reference it using /proc/self/fd/0.

CVE-2017-17692

- Samsung Internet Browser 5.4.02.3 allows remote attackers to bypass the Same Origin Policy and obtain sensitive information via crafted JavaScript code that redirects to a child tab and rewrites the innerHTML property.

CVE-2017-17867

- Inteno iopsys 2.0-3.14 and 4.0 devices allow remote authenticated users to execute arbitrary OS commands by modifying the leasetrigger field in the odhcpd configuration to specify an arbitrary program, as demonstrated by a

program located on an SMB share. This issue existed because the /etc/uci-defaults directory was not being used to secure the OpenWrt configuration.

CVE-2017-17969

- Heap-based buffer overflow in the NCompress::NShrink::CDecoder::CodeReal method in 7-Zip before 18.00 and p7zip allows remote attackers to cause a denial of service (out-of-bounds write) or potentially execute arbitrary code via a crafted ZIP archive.

CVE-2017-1000112

- Exploitable memory corruption due to UFO to non-UFO path switch.

CVE-2017-1000117

- A malicious third-party can give a crafted "ssh://..." URL to an unsuspecting victim, and an attempt to visit the URL can result in any program that exists on the victim's machine being executed. Such a URL could be placed in the .gitmodules file of a malicious project, and an unsuspecting victim could be tricked into running "git clone --recurse-submodules" to trigger the vulnerability.

CVE-2017-1000251

- The native Bluetooth stack in the Linux Kernel (BlueZ), starting at the Linux kernel version 3.3-rc1 and up to and including 4.13.1, are vulnerable to a stack overflow vulnerability in the processing of L2CAP configuration responses resulting in Remote code execution in kernel space.

CVE-2017-1000353

- Jenkins Java Deserialization CVE-2017-1000353 Remote Code Execution Vulnerability.

CVE-2017-1000364

- An issue was discovered in the size of the stack guard page on Linux, specifically a 4k stack guard page is not sufficiently large and can be "jumped" over (the stack guard page is bypassed), this affects Linux Kernel versions 4.11.5 and earlier (the stackguard page was introduced in 2010).

CVE-2017-1000365

- The Linux Kernel imposes a size restriction on the arguments and environmental strings passed through RLIMIT_STACK/RLIM_INFINITY (1/4 of the size), but does not take the argument and environment pointers into account, which allows attackers to bypass this limitation. This affects Linux Kernel versions 4.11.5 and earlier. It appears that this feature was introduced in the Linux Kernel version 2.6.23.

CVE-2017-1000366

- glibc contains a vulnerability that allows specially crafted LD_LIBRARY_PATH values to manipulate the heap/stack, causing them to alias, potentially resulting in arbitrary code execution. Please note that additional hardening changes have been made to glibc to prevent manipulation of stack and heap memory but these issues are not directly exploitable, as such they have not been given a CVE. This affects glibc 2.25 and earlier.

CVE-2017-1000367

- A vulnerability in Sudo's get_process_ttyname() for Linux: this function opens "/proc/[pid]/stat" (man proc) and reads the device number of the tty from field 7 (tty_nr). Unfortunately, these fields are space-separated and field 2 (comm, the filename of the command) can contain spaces (CVE-2017-1000367).

CVE-2017-1000369

- Exim supports the use of multiple "-p" command line arguments which are malloc()'ed and never free()'ed, used in conjunction with other issues allows attackers to cause arbitrary code execution. This affects exim version 4.89 and earlier. Please note that at this time upstream has released a patch (commit 65e061b76867a9ea7aeeb535341b790b90ae6c21), but it is not known if a new point release is available that addresses this issue at this time.

CVE-2017-1000370

- The offset2lib patch as used in the Linux Kernel contains a vulnerability that allows a PIE binary to be execve()'ed with 1GB of arguments or environmental strings then the stack occupies the address 0x80000000 and the PIE binary is mapped above 0x40000000 nullifying the protection of the offset2lib patch. This affects Linux Kernel version 4.11.5 and earlier. This is a different issue than CVE-2017-1000371. This issue appears to be limited to i386 based systems.

CVE-2017-1000371

- The offset2lib patch as used by the Linux Kernel contains a vulnerability, if RLIMIT_STACK is set to RLIM_INFINITY and 1 Gigabyte of memory is allocated (the maximum under the 1/4 restriction) then the stack will be grown down to 0x80000000, and as the PIE binary is mapped above 0x80000000 the minimum distance between the end of the PIE binary's read-write segment and the start of the stack becomes small enough that the stack guard page can be jumped over by an attacker. This affects Linux Kernel version 4.11.5. This is a different issue than CVE-2017-1000370 and CVE-2017-1000365. This issue appears to be limited to i386 based systems.

CVE-2017-1000372

- A flaw exists in OpenBSD's implementation of the stack guard page that allows attackers to bypass it resulting in arbitrary code execution using setuid binaries such as /usr/bin/at. This affects OpenBSD 6.1 and possibly earlier versions.

CVE-2017-1000373

- The OpenBSD qsort() function is recursive, and not randomized, an attacker can construct a pathological input array of N elements that causes qsort() to deterministically recurse N/4 times. This allows attackers to consume arbitrary amounts of stack memory and manipulate stack memory to assist in arbitrary code execution attacks. This affects OpenBSD 6.1 and possibly earlier versions.

CVE-2017-1000374

- A flaw exists in NetBSD's implementation of the stack guard page that allows attackers to bypass it resulting in arbitrary code execution using certain setuid binaries. This affects NetBSD 7.1 and possibly earlier versions.

CVE-2017-1000375

- NetBSD maps the run-time link-editor ld.so directly below the stack region, even if ASLR is enabled, this allows attackers to more easily manipulate memory leading to arbitrary code execution. This affects NetBSD 7.1 and possibly earlier versions.

CVE-2017-1000376

- libffi requests an executable stack allowing attackers to more easily trigger arbitrary code execution by overwriting the stack. Please note that libffi is used by a number of other libraries. It was previously stated that this affects libffi version 3.2.1 but this appears to be incorrect. libffi prior to version 3.1 on 32 bit x86 systems was vulnerable, and upstream is believed to have fixed this issue in version 3.1.

CVE-2017-1000377

- An issue was discovered in the size of the default stack guard page on PAX Linux (originally from GRSecurity but shipped by other Linux vendors), specifically the default stack guard page is not sufficiently large and can be "jumped" over (the stack guard page is bypassed), this affects PAX Linux Kernel versions as of June 19, 2017 (specific version information is not available at this time).

CVE-2017-1000378

- The NetBSD qsort() function is recursive, and not randomized, an attacker can construct a pathological input array of N elements that causes qsort() to deterministically recurse N/4 times. This allows attackers to consume arbitrary amounts of stack memory and manipulate stack memory to assist in arbitrary code execution attacks. This affects NetBSD 7.1 and possibly earlier versions.

CVE-2017-1000379

- The Linux Kernel running on AMD64 systems will sometimes map the contents of PIE executable, the heap or ld.so to where the stack is mapped allowing attackers to more easily manipulate the stack. Linux Kernel version 4.11.5 is affected.

CVE-2017-1000405

- The Linux Kernel versions 2.6.38 through 4.14 have a problematic use of pmd_mkdirty() in the touch_pmd() function inside the THP implementation. touch_pmd() can be reached by get_user_pages(). In such case, the pmd will become dirty. This scenario breaks the new can_follow_write_pmd()'s logic - pmd can become dirty without going through a COW cycle. This bug is not as severe as the original "Dirty cow" because an ext4 file (or any other regular file) cannot be mapped using THP. Nevertheless, it does allow us to overwrite read-only huge pages. For example, the zero huge page and sealed shmem files can be overwritten (since their mapping can be populated using THP). Note that after the first write page-fault to the zero page, it will be replaced with a new fresh (and zeroed) thp.

CVE-2017-1000424

- Github Electron version 1.6.4 - 1.6.11 and 1.7.0 - 1.7.5 is vulnerable to a URL Spoofing problem when opening PDFs in PDFium resulting loading arbitrary PDFs that a hacker can control.

CVE-2017-1000459

- Leanote version <= 2.5 is vulnerable to XSS due to not sanitized input in markdown notes.

CVE-2017-1002101

- In Kubernetes versions 1.3.x, 1.4.x, 1.5.x, 1.6.x and prior to versions 1.7.14, 1.8.9 and 1.9.4 containers using subpath volume mounts with any volume type (including non-privileged pods, subject to file permissions) can access files/directories outside of the volume, including the host's filesystem.

CVE-2018-0101

- A vulnerability in the Secure Sockets Layer (SSL) VPN functionality of the Cisco Adaptive Security Appliance (ASA) Software could allow an unauthenticated, remote attacker to cause a reload of the affected system or to remotely execute code. The vulnerability is due to an attempt to double free a region of memory when the webvpn feature is enabled on the Cisco ASA device. An attacker could exploit this vulnerability by sending multiple, crafted XML packets to a webvpn-configured interface on the affected system. An exploit could allow the attacker to execute arbitrary code and obtain full control of the system, or cause a reload of the affected device. This vulnerability affects Cisco ASA Software that is running on the following Cisco products: 3000 Series Industrial Security Appliance (ISA), ASA 5500 Series Adaptive Security Appliances, ASA 5500-X Series Next-Generation Firewalls, ASA Services Module for Cisco Catalyst 6500 Series Switches and Cisco 7600 Series Routers, ASA 1000V Cloud Firewall, Adaptive Security Virtual Appliance (ASAv), Firepower 2100 Series Security Appliance, Firepower 4110 Security Appliance, Firepower 9300 ASA Security Module, Firepower Threat Defense Software (FTD). Cisco Bug IDs: CSCvg35618.

CVE-2018-0114

- A vulnerability in the Cisco node-jose open source library before 0.11.0 could allow an unauthenticated, remote attacker to re-sign tokens using a key that is embedded within the token. The vulnerability is due to node-jose following the JSON Web Signature (JWS) standard for JSON Web Tokens (JWTs). This standard specifies that a JSON Web Key (JWK) representing a public key can be embedded within the header of a JWS. This public key is then trusted for verification. An attacker could exploit this by forging valid JWS objects by removing the original signature, adding a new public key to

the header, and then signing the object using the (attacker-owned) private key associated with the public key embedded in that JWS header.

CVE-2018-0171

- A vulnerability in the Smart Install feature of Cisco IOS Software and Cisco IOS XE Software could allow an unauthenticated, remote attacker to trigger a reload of an affected device, resulting in a denial of service (DoS) condition, or to execute arbitrary code on an affected device. The vulnerability is due to improper validation of packet data. An attacker could exploit this vulnerability by sending a crafted Smart Install message to an affected device on TCP port 4786. A successful exploit could allow the attacker to cause a buffer overflow on the affected device, which could have the following impacts: Triggering a reload of the device, Allowing the attacker to execute arbitrary code on the device, Causing an indefinite loop on the affected device that triggers a watchdog crash. Cisco Bug IDs: CSCvg76186.

CVE-2018-0492

- Johnathan Nightingale beep through 1.3.4, if setuid, has a race condition that allows local privilege escalation.

CVE-2018-0743

- Windows Subsystem for Linux in Windows 10 version 1703, Windows 10 version 1709, and Windows Server, version 1709 allows an elevation of privilege vulnerability due to the way objects are handled in memory, aka "Windows Subsystem for Linux Elevation of Privilege Vulnerability".

CVE-2018-0744

- The Windows kernel in Windows 8.1 and RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703 and 1709, Windows Server 2016 and Windows Server, version 1709 allows an elevation of privilege vulnerability due to the way objects are handled in memory, aka "Windows Elevation of Privilege Vulnerability".

CVE-2018-0752

- The Windows Kernel API in Windows 8.1 and RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703 and 1709, Windows Server 2016 and Windows Server, version 1709 allows an elevation of privilege vulnerability due to the way the Kernel API enforces permissions, aka "Windows Elevation of Privilege Vulnerability". This CVE ID is unique from CVE-2018-0751.

CVE-2018-0758

- Microsoft Edge in Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2018-0762, CVE-2018-0768, CVE-2018-0769, CVE-2018-0770, CVE-2018-0772, CVE-2018-0773, CVE-2018-0774, CVE-2018-0775, CVE-2018-0776, CVE-2018-0777, CVE-2018-0778, and CVE-2018-0781.

CVE-2018-0763

- Microsoft Edge in Microsoft Windows 10 1703 and 1709 allows information disclosure, due to how Edge handles objects in memory, aka "Microsoft Edge Information Disclosure Vulnerability". This CVE ID is unique from CVE-2018-0839.

CVE-2018-0767

- Microsoft Edge in Microsoft Windows 10 1511, 1607, 1703, 1709, and Windows Server 2016 allows an attacker to obtain information to further compromise the user's system, due to how the scripting engine handles objects in memory, aka "Scripting Engine Information Disclosure Vulnerability". This CVE ID is unique from CVE-2018-0780 and CVE-2018-0800.

CVE-2018-0769

- Microsoft Edge in Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2018-0758, CVE-2018-0762, CVE-2018-0768, CVE-2018-0770, CVE-2018-0772, CVE-2018-0773, CVE-2018-0774, CVE-2018-0775, CVE-2018-0776, CVE-2018-0777, CVE-2018-0778, and CVE-2018-0781.

CVE-2018-0770

- Microsoft Edge in Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2018-0758, CVE-2018-0762, CVE-2018-0768, CVE-2018-0769, CVE-2018-0772, CVE-2018-0773, CVE-2018-0774, CVE-2018-0775, CVE-2018-0776, CVE-2018-0777, CVE-2018-0778, and CVE-2018-0781.

CVE-2018-0774

- Microsoft Edge in Windows 10 1709 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2018-0758, CVE-2018-0762, CVE-2018-0768, CVE-2018-0769, CVE-2018-0770, CVE-2018-0772, CVE-2018-0773, CVE-2018-0775, CVE-2018-0776, CVE-2018-0777, CVE-2018-0778, and CVE-2018-0781.

CVE-2018-0775

- Microsoft Edge in Windows 10 1709 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2018-0758, CVE-2018-0762, CVE-2018-0768, CVE-2018-0769, CVE-2018-0770, CVE-2018-0772, CVE-2018-0773, CVE-2018-0774, CVE-2018-0776, CVE-2018-0777, CVE-2018-0778, and CVE-2018-0781.

CVE-2018-0776

- Microsoft Edge in Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2018-0758, CVE-2018-0762, CVE-2018-0768, CVE-2018-0769, CVE-2018-0770, CVE-2018-0772, CVE-2018-0773, CVE-2018-0774, CVE-2018-0775, CVE-2018-0777, CVE-2018-0778, and CVE-2018-0781.

CVE-2018-0777

- Microsoft Edge in Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2018-0758, CVE-2018-0762, CVE-2018-0768, CVE-2018-0769, CVE-2018-0770, CVE-2018-0772, CVE-2018-0773, CVE-2018-0774, CVE-2018-0775, CVE-2018-0776, CVE-2018-0778, and CVE-2018-0781.

CVE-2018-0780

- Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows an attacker to obtain information to further compromise the user's system, due to how the scripting engine handles objects in memory, aka "Scripting Engine Information Disclosure Vulnerability". This CVE ID is unique from CVE-2018-0767 and CVE-2018-0800.

CVE-2018-0797

- Microsoft Office 2010, Microsoft Office 2013, and Microsoft Office 2016 allow a remote code execution vulnerability due to the way RTF content is handled, aka "Microsoft Word Memory Corruption Vulnerability".

CVE-2018-0802

- Equation Editor in Microsoft Office 2007, Microsoft Office 2010, Microsoft Office 2013, and Microsoft Office 2016 allow a remote code execution vulnerability due to the way objects are handled in memory, aka "Microsoft Office Memory Corruption Vulnerability". This CVE is unique from CVE-2018-0797 and CVE-2018-0812.

CVE-2018-0833

- The Microsoft Server Message Block 2.0 and 3.0 (SMBv2/SMBv3) client in Windows 8.1 and RT 8.1 and Windows Server 2012 R2 allows a denial of service vulnerability due to how specially crafted requests are handled, aka "SMBv2/SMBv3 Null Dereference Denial of Service Vulnerability".

CVE-2018-0834

- Microsoft Edge and ChakraCore in Microsoft Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows remote code execution, due to how the scripting engine handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2018-0835, CVE-2018-0836, CVE-2018-0837, CVE-2018-0838, CVE-2018-0840, CVE-2018-0856, CVE-2018-0857, CVE-2018-0858, CVE-2018-0859, CVE-2018-0860, CVE-2018-0861, and CVE-2018-0866.

CVE-2018-0835

- Microsoft Edge and ChakraCore in Microsoft Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows remote code execution, due to how the scripting engine handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2018-0834, CVE-2018-0836, CVE-2018-0837, CVE-2018-0838, CVE-2018-0840, CVE-2018-0856, CVE-2018-0857, CVE-2018-0858, CVE-2018-0859, CVE-2018-0860, CVE-2018-0861, and CVE-2018-0866.

CVE-2018-0837

- Microsoft Edge and ChakraCore in Microsoft Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows remote code execution, due to how the scripting engine handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2018-0834, CVE-2018-0835, CVE-2018-0836, CVE-2018-0838, CVE-2018-0840, CVE-2018-0856, CVE-2018-0857, CVE-2018-0858, CVE-2018-0859, CVE-2018-0860, CVE-2018-0861, and CVE-2018-0866.

CVE-2018-0838

- Microsoft Edge and ChakraCore in Microsoft Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows remote code execution, due to how the scripting engine handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2018-0834, CVE-2018-0835, CVE-2018-0836, CVE-2018-0837, CVE-2018-0840, CVE-2018-0856, CVE-2018-0857, CVE-2018-0858, CVE-2018-0859, CVE-2018-0860, CVE-2018-0861, and CVE-2018-0866.

CVE-2018-0840

- Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, and Internet Explorer and Microsoft Edge in Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows remote code execution, due to how the scripting engine handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2018-0834, CVE-2018-0835, CVE-2018-0836, CVE-2018-0837, CVE-2018-0838, CVE-2018-0856, CVE-2018-0857, CVE-2018-0858, CVE-2018-0859, CVE-2018-0860, CVE-2018-0861, and CVE-2018-0866.

CVE-2018-0860

- Microsoft Edge and ChakraCore in Microsoft Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows remote code execution, due to how the scripting engine handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2018-0834, CVE-2018-0835, CVE-2018-0836, CVE-

2018-0837, CVE-2018-0838, CVE-2018-0840, CVE-2018-0856, CVE-2018-0857, CVE-2018-0858, CVE-2018-0859, CVE-2018-0861, and CVE-2018-0866.

CVE-2018-0878

- Windows Remote Assistance in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1 and RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, and 1709, Windows Server 2016 and Windows Server, version 1709 allows an information disclosure vulnerability due to how XML External Entities (XXE) are processed, aka "Windows Remote Assistance Information Disclosure Vulnerability".

CVE-2018-0886

- The Credential Security Support Provider protocol (CredSSP) in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1 and RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, and 1709 Windows Server 2016 and Windows Server, version 1709 allows a remote code execution vulnerability due to how CredSSP validates request during the authentication process, aka "CredSSP Remote Code Execution Vulnerability".

CVE-2018-0891

- ChakraCore, and Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, and Internet Explorer and Microsoft Edge in Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allow information disclosure, due to how the scripting engine handles objects in memory, aka "Scripting Engine Information Disclosure Vulnerability". This CVE ID is unique from CVE-2018-0939.

CVE-2018-0933

- ChakraCore and Microsoft Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows remote code execution, due to how the Chakra scripting engine handles objects in memory, aka "Chakra Scripting Engine Memory

Corruption Vulnerability". This CVE ID is unique from CVE-2018-0872, CVE-2018-0873, CVE-2018-0874, CVE-2018-0930, CVE-2018-0931, CVE-2018-0934, CVE-2018-0936, and CVE-2018-0937.

CVE-2018-0934

- ChakraCore and Microsoft Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows remote code execution, due to how the Chakra scripting engine handles objects in memory, aka "Chakra Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2018-0872, CVE-2018-0873, CVE-2018-0874, CVE-2018-0930, CVE-2018-0931, CVE-2018-0933, CVE-2018-0936, and CVE-2018-0937.

CVE-2018-1037

- An information disclosure vulnerability exists when Visual Studio improperly discloses limited contents of uninitialized memory while compiling program database (PDB) files, aka "Microsoft Visual Studio Information Disclosure Vulnerability." This affects Microsoft Visual Studio.

CVE-2018-1038

- The Windows kernel in Windows 7 SP1 and Windows Server 2008 R2 SP1 allows an elevation of privilege vulnerability due to the way it handles objects in memory, aka "Windows Kernel Elevation of Privilege Vulnerability."

CVE-2018-1270

- Spring Framework, versions 5.0 prior to 5.0.5 and versions 4.3 prior to 4.3.15 and older unsupported versions, allow applications to expose STOMP over WebSocket endpoints with a simple, in-memory STOMP broker through the spring-messaging module. A malicious user (or attacker) can craft a message to the broker that can lead to a remote code execution attack.

CVE-2018-1273

- Spring Data Commons, versions prior to 1.13 to 1.13.10, 2.0 to 2.0.5, and older unsupported versions, contain a property binder vulnerability caused by improper neutralization of special elements. An unauthenticated remote malicious user (or attacker) can supply specially crafted request parameters against Spring Data REST backed HTTP resources or using Spring Data's projection-based request payload binding that can lead to a remote code execution attack.

CVE-2018-1275

- Spring Framework, versions 5.0 prior to 5.0.5 and versions 4.3 prior to 4.3.16 and older unsupported versions, allow applications to expose STOMP over WebSocket endpoints with a simple, in-memory STOMP broker through the spring-messaging module. A malicious user (or attacker) can craft a message to the broker that can lead to a remote code execution attack. This CVE addresses the partial fix for CVE-2018-1270 in the 4.3.x branch of the Spring Framework.

CVE-2018-2628

- Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: WLS Core Components). Supported versions that are affected are 10.3.6.0, 12.1.3.0, 12.2.1.2 and 12.2.1.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3 to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.0 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).

CVE-2018-2694

- Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are Prior to 5.1.32 and Prior to 5.2.6. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.0 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).

CVE-2018-2698

- Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are Prior to 5.1.32 and Prior to 5.2.6. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.0 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).

CVE-2018-4087

- An issue was discovered in certain Apple products. iOS before 11.2.5 is affected. tvOS before 11.2.5 is affected. watchOS before 4.2.2 is affected. The issue involves the "Core Bluetooth" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app.

CVE-2018-4121

- An issue was discovered in certain Apple products. iOS before 11.3 is affected. Safari before 11.1 is affected. iCloud before 7.4 on Windows is affected. iTunes before 12.7.4 on Windows is affected. tvOS before 11.3 is affected. watchOS before 4.3 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.

CVE-2018-4148

- An issue was discovered in certain Apple products. iOS before 11.3 is affected. The issue involves the "Telephony" component. A buffer overflow allows remote attackers to execute arbitrary code.

CVE-2018-4150

- An issue was discovered in certain Apple products. iOS before 11.3 is affected. macOS before 10.13.4 is affected. tvOS before 11.3 is affected. watchOS before 4.3 is affected. The issue involves the "Kernel" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app.

CVE-2018-4878

- A use-after-free vulnerability was discovered in Adobe Flash Player before 28.0.0.161. This vulnerability occurs due to a dangling pointer in the Primetime SDK related to the handling of listener objects. A successful attack can lead to arbitrary code execution. This was exploited in the wild in January and February 2018.

CVE-2018-5146

- **** RESERVED **** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.

CVE-2018-5181

- **** RESERVED **** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.

CVE-2018-5189

- Race condition in Jungo Windriver 12.5.1 allows local users to cause a denial of service (buffer overflow) or gain system privileges by flipping pool buffer size, aka a "double fetch" vulnerability.

CVE-2018-5318

- **** RESERVED **** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.

CVE-2018-5711

- `gd_gif_in.c` in the GD Graphics Library (aka `libgd`), as used in PHP before 5.6.33, 7.0.x before 7.0.27, 7.1.x before 7.1.13, and 7.2.x before 7.2.1, has an integer signedness error that leads to an infinite loop via a crafted GIF file, as demonstrated by a call to the `imagecreatefromgif` or `imagecreatefromstring` PHP function. This is related to `GetCode_` and `gdImageCreateFromGifCtx`.

CVE-2018-5996

- Insufficient exception handling in the method `NCompress::NRar3::CDecoder::Code` of 7-Zip before 18.00 and p7zip can lead to multiple memory corruptions within the PPMd code, allows remote attackers to cause a denial of service (segmentation fault) or execute arbitrary code via a crafted RAR archive.

CVE-2018-6034

- **** RESERVED **** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.

CVE-2018-6055

- **** RESERVED **** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.

CVE-2018-6072

- **** RESERVED **** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.

CVE-2018-6184

- ZEIT Next.js 4 before 4.2.3 has Directory Traversal under the /_next request namespace.

CVE-2018-6317

- The remote management interface in Claymore Dual Miner 10.5 and earlier is vulnerable to an unauthenticated format string vulnerability, allowing remote attackers to read memory or cause a denial of service.

CVE-2018-6376

- In Joomla! before 3.8.4, the lack of type casting of a variable in a SQL statement leads to a SQL injection vulnerability in the Hathor postinstall message.

CVE-2018-6389

- In WordPress through 4.9.2, unauthenticated attackers can cause a denial of service (resource consumption) by using the large list of registered .js files (from wp-includes/script-loader.php) to construct a series of requests to load every file many times.

CVE-2018-6460

- Hotspot Shield runs a webserver with a static IP address 127.0.0.1 and port 895. The web server uses JSONP and hosts sensitive information including configuration. User controlled input is not sufficiently filtered: an unauthenticated attacker can send a POST request to /status.js with the parameter func=\$_APPLOG.Rfunc and extract sensitive information about the machine, including whether the user is connected to a VPN, to which VPN he/she is connected, and what is their real IP address.

CVE-2018-6789

- An issue was discovered in the base64d function in the SMTP listener in Exim before 4.90.1. By sending a handcrafted message, a buffer overflow may happen. This can be used to execute code remotely.

CVE-2018-6794

- Suricata before 4.1 is prone to an HTTP detection bypass vulnerability in detect.c and stream-tcp.c. If a malicious server breaks a normal TCP flow and sends data before the 3-way handshake is complete, then the data sent by the malicious server will be accepted by web clients such as a web browser or Linux CLI utilities, but ignored by Suricata IDS signatures. This mostly affects IDS signatures for the HTTP protocol and TCP stream content; signatures for TCP packets will inspect such network traffic as usual.

CVE-2018-6871

- LibreOffice through 6.0.1 allows remote attackers to read arbitrary files via =WEBSERVICE calls in a document, which use the COM.MICROSOFT.WEBSERVICE function.

CVE-2018-7260

- Cross-site scripting (XSS) vulnerability in db_central_columns.php in phpMyAdmin before 4.7.8 allows remote authenticated users to inject arbitrary web script or HTML via a crafted URL.

CVE-2018-7273

- In the Linux kernel through 4.15.4, the floppy driver reveals the addresses of kernel functions and global variables using printk calls within the function show_floppy in drivers/block/floppy.c. An attacker can read this information from dmesg and use the addresses to find the locations of kernel code and data and bypass kernel security protections such as KASLR.

CVE-2018-7600

- Drupal before 7.58, 8.x before 8.3.9, 8.4.x before 8.4.6, and 8.5.x before 8.5.1 allows remote attackers to execute arbitrary code because of an issue affecting multiple subsystems with default or common module configurations.

CVE-2018-7602

- **** RESERVED **** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.

CVE-2018-8719

- An issue was discovered in the WP Security Audit Log plugin 3.1.1 for WordPress. Access to wp-content/uploads/wp-security-audit-log/* files is not restricted. For example, these files are indexed by Google and allows for attackers to possibly find sensitive information.

CVE-2018-8733

- Authentication bypass vulnerability in the core config manager in Nagios XI 5.2.x through 5.4.x before 5.4.13 allows an unauthenticated attacker to make configuration changes and leverage an authenticated SQL injection vulnerability.

CVE-2018-8734

- SQL injection vulnerability in the core config manager in Nagios XI 5.2.x through 5.4.x before 5.4.13 allows an attacker to execute arbitrary SQL commands via the sellInfoKey1 parameter.

CVE-2018-8735

- Remote command execution (RCE) vulnerability in Nagios XI 5.2.x through 5.4.x before 5.4.13 allows an attacker to execute arbitrary commands on the target system, aka OS command injection.

CVE-2018-8736

- A privilege escalation vulnerability in Nagios XI 5.2.x through 5.4.x before 5.4.13 allows an attacker to leverage an RCE vulnerability escalating to root.

CVE-2018-8778

- In Ruby before 2.2.10, 2.3.x before 2.3.7, 2.4.x before 2.4.4, 2.5.x before 2.5.1, and 2.6.0-preview1, an attacker controlling the unpacking format (similar to format string vulnerabilities) can trigger a buffer under-read in the String#unpack method, resulting in a massive and controlled information disclosure.

CVE-2018-8897

- A statement in the System Programming Guide of the Intel 64 and IA-32 Architectures Software Developer's Manual (SDM) was mishandled in the development of some or all operating-system kernels, resulting in unexpected behavior for #DB exceptions that are deferred by MOV SS or POP SS, as demonstrated by (for example) privilege escalation in Windows, macOS, some Xen configurations, or FreeBSD, or a Linux kernel crash. The MOV to SS and POP SS instructions inhibit interrupts (including NMIs), data breakpoints, and single step trap exceptions until the instruction boundary following the next instruction (SDM Vol. 3A; section 6.8.3). (The inhibited data breakpoints are those on memory accessed by the MOV to SS or POP to SS instruction itself.) Note that debug exceptions are not inhibited by the interrupt enable (EFLAGS.IF) system flag (SDM Vol. 3A; section 2.3). If the instruction following the MOV to SS or POP to SS instruction is an instruction like SYSCALL, SYSENTER, INT 3, etc. that transfers control to the operating system at CPL < 3, the debug exception is delivered after the transfer to CPL < 3 is complete. OS kernels may not expect this order of events and may therefore experience unexpected behavior when it occurs.

CVE-2018-9995

- TBK DVR4104 and DVR4216 devices allow remote attackers to bypass authentication via a "Cookie: uid=admin" header, as demonstrated by a device.rsp?opt=user&cmd=list request that provides credentials within JSON data in a response.

CVE-2018-10115

- **** RESERVED **** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.

CVE-2018-10172

- 7-Zip through 18.01 on Windows implements the "Large memory pages" option by calling the LsaAddAccountRights function to add the SeLockMemoryPrivilege privilege to the user's account, which makes it easier for attackers to bypass intended access restrictions by using this privilege in the context of a sandboxed process.

CVE-2018-10561

- **** RESERVED **** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.

CVE-2018-10562

- **** RESERVED **** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.

CVE-2018-10641

- D-Link DIR-601 A1 1.02NA devices do not require the old password for a password change, which occurs in cleartext.

CVE-2018-10676

- CeNova, Night OWL, Novo, Pulnix, QSee, Securus, and TBK Vision DVR devices allow remote attackers to download a file and obtain sensitive credential information via a direct request for the download.rsp URI.

CVE-2018-1000006

- GitHub Electron versions 1.8.2-beta.3 and earlier, 1.7.10 and earlier, 1.6.15 and earlier has a vulnerability in the protocol handler, specifically Electron apps running on Windows 10, 7 or 2008 that register custom protocol handlers can be tricked in arbitrary command execution if the user clicks on a specially crafted URL. This has been fixed in versions 1.8.2-beta.4, 1.7.11, and 1.6.16.

CVE-2018-1000129

- An XSS vulnerability exists in the Jolokia agent version 1.3.7 in the HTTP servlet that allows an attacker to execute malicious javascript in the victim's browser.

CVE-2018-1000130

- A JNDI Injection vulnerability exists in Jolokia agent version 1.3.7 in the proxy mode that allows a remote attacker to run arbitrary Java code on the server.

CVE-2018-1000136

- Electron version 1.7 up to 1.7.12; 1.8 up to 1.8.3 and 2.0.0 up to 2.0.0-beta.3 contains an improper handling of values vulnerability in Webviews that can result in remote code execution. This attack appear to be exploitable via an app which allows execution of 3rd party code AND disallows node integration AND has not specified if webview is enabled/disabled. This vulnerability appears to have been fixed in 1.7.13, 1.8.4, 2.0.0-beta.4.

Code of Conduct

Please note that this project is released with a [Contributor Code of Conduct](#). By participating in this project you agree to abide by its terms.

License



To the extent possible under law, [@qazbnm456](#) has waived all copyright and related or neighboring rights to this work.

