McAfee Exploit Prevention Content 8537

Release Notes | 2018-07-10

Content package version for -

McAfee Host Intrusion Prevention: 8.0.0.8537

McAfee Endpoint Security Exploit Prevention: 10.6.0.8537

Below is the updated signature information for the McAfee Exploit Prevention content.

New Windows Signatures	Minimum Supported Product version	
	Host Intrusion Prevention	Endpoint Security Exploit Prevention
Signature 6118: *Fileless Threat: Malicious Code Execution using DotNetToJScript Technique* *Description:* - *This event indicates an attempt to execute malicious shellcode using DotNetToJScript Technique, which is used by prevalent fileless malwares like CACTUSTORCH. DotNetToJScript attack vectors allow loading and execution of malicious .NET assembly (DLL, EXE etc.) straight from memory with the help of .NET libraries exposed via COM. Just like any other typical file-less attack technique, DotNetToJScript does not write any part of the malicious .NET DLL or EXE in the computer's hard drive.* - *This signature is set to level Low by default* *Note: Customer can change the level / reaction-type of this signature based on their requirement.*	*8.0.0*	*10.5.0*

Note: Refer to the KB for the default Reaction-type associated with Signature severity level for all supported Product versions: https://kc.mcafee.com/corporate/index?page=content&id=KB90369

Updated Windows Signatures	Minimum Supported Product version	
	Host Intrusion Prevention	Endpoint Security Exploit Prevention

BugFix: *The following signatures have been Disabled by default as the platforms affected by the corresponding vulnerabilities are out of scope for Endpoint Security product*

Signature ID	***Signature Name***	***Vulnerability Information***
2231	Vulnerability in SMB Could Allow Remote Code Execution	CVE-2009-3103
2232	SMB Buffer Overflow Remote Code Execution Vulnerability	CVE-2008-4834
2233	SMB Validation Remote Code Execution Vulnerability	CVE-2008-4835
3718	Network Share Provider Denial of Service (SMBdie)	CVE-2002-0724
3720	MSSQL Resolution Service Buffer Overflow (Slammer)	CVE-2002-0649
3721	RPC DCOM Stack Buffer Overflow (Blaster, Nachi)	CVE-2003-0352
3722	RPC Service Denial of Service (WinNuke)	CVE-2002-1561
3723	Windows PPTP Server Buffer Overflow	CVE-2002-1214
3724	LSASS Dcpromo Log File Buffer Overflow (Sasser)	CVE-2003-0533
3725	IP Options Validation Overflow	CVE-2005-0048
3801	Vulnerability in TCP/IP Could Allow Remote Code Execution	CVE-2006-2379
3802	Vulnerability in Server Service Could Allow Remote Code Execution	CVE-2006-1314
3803	Vulnerabilities in DNS Resolution Could Allow Remote Code Execution	CVE-2006-3441
3804	Vulnerability in Server Service Could Allow Denial of Service	CVE-2006-3942
3806	FTP Username/Password Overflow	CVE-1999-0256
3845	Vulnerability in Universal Plug and Play (UPnP) Service Could Allow Remote Code Execution	CVE-2007-1204
3846	Vulnerability in processing FTP Reply Could Allow Remote Code Execution	CVE-2007-0217
6029	SMB Buffer Underflow Vulnerability	CVE-2008-4038

Note: This change is not applicable for Host Intrusion Prevention product.

The above listed signatures will be deprecated in future content releases as the vulnerabilities are not applicable for the Supported platforms of Endpoint Security product.

Please refer to the below KB for the list of Platforms supported by Endpoint Security Product

https://kc.mcafee.com/corporate/index?page=content&id=KB82761

NA

10.5.3

Existing coverage for New Vulnerabilities	Minimum Supported Product version	
	Host Intrusion Prevention	Endpoint Security Exploit Prevention
Coverage by GBOP: *GBOP Signatures 428, 1146, 6012, 6013, 6014 and 6048 are expected to cover the below vulnerabilities:* - *CVE-2018-8242* - *CVE-2018-8296*	*8.0.0*	*10.2.0*
Coverage by GBOP: *GBOP Signatures 428, 6012, 6013, 6014 and 6048 are expected to cover the below vulnerabilities:* - *CVE-2018-5007* - *CVE-2018-5009* - *CVE-2018-5011* - *CVE-2018-5015* - *CVE-2018-5020* - *CVE-2018-5021* - *CVE-2018-5034* - *CVE-2018-5036* - *CVE-2018-5037* - *CVE-2018-5040* - *CVE-2018-5041* - *CVE-2018-5043* - *CVE-2018-5045* - *CVE-2018-5052* - *CVE-2018-5058* - *CVE-2018-5059* - *CVE-2018-5064* - *CVE-2018-5065* - *CVE-2018-5067* - *CVE-2018-5069* - *CVE-2018-5070* - *CVE-2018-12754* - *CVE-2018-12755* - *CVE-2018-12756* - *CVE-2018-12758* - *CVE-2018-12760* - *CVE-2018-12770* - *CVE-2018-12771* - *CVE-2018-12772* - *CVE-2018-12773* - *CVE-2018-12776* - *CVE-2018-12782* - *CVE-2018-12783*	*8.0.0*	*10.2.0*

- *CVE-2018-12784* - *CVE-2018-12785* - *CVE-2018-12787* - *CVE-2018-12791* - *CVE-2018-12796* - *CVE-2018-12798*		
Coverage by GPEP: *Generic Privilege Escalation Prevention (Signature 6052) is expected to cover the below vulnerabilities:* - *CVE-2018-8282*	*8.0.0*	*10.2.0*

How to Update

You need to check in the update package to the ePO Repository, and then send the updated information to the agents. Please refer to 'Updating' in Chapter 8 of 'Host Intrusion Prevention Product Guide'