Vulnerability Based Current Status Report

2019-08-27 20:20:02

Current State

30

System Base Risk Score

6 / 74

Vulnerability (Distinct / Total)

8

Subnet

18

Device

105

Software

74

Port Service

Reported Vulnerabilities

No	Title/Definition	Device Count	Subnet Count	Location Count	Business Unit Count	Base Risk Score	Exploitability
CVE-2014-6271	GNU Bash CVE-2014-6271 Remote Code Execution Vulnerability	4	4	0	1	100	Exist
CVE-2017-0148	Microsoft Windows SMB Server CVE-2017-0148 Remote Code Execution	14	6	0	0	90	Exist
CVE-2017-0146	Microsoft Windows SMB Server CVE-2017-0146 Remote Code Execution	14	6	0	0	90	Exist
CVE-2017-0145	Microsoft Windows SMB Server CVE-2017-0145 Remote Code Execution	14	6	0	0	90	Exist
CVE-2017-0144	Microsoft Windows SMB Server CVE-2017-0144 Remote Code Execution	14	6	0	0	90	Exist
CVE-2017-0143	Microsoft Windows SMB Server CVE-2017-0143 Remote Code Execution	14	6	0	0	90	Exist

CVE-2014-6271 - GNU Bash CVE-2014-6271 Remote Code Execution Vulnerability

100 (Critical Risk)	Exist	4	4	0	1
Base Risk	Exploitability	Device Count	Subnet Count	Location Count	Business Unit

Publish Date : 2014-09-24 15:48:04

Last Modified Date : 2019-08-27 16:21:39

Impact Values

Importance Level : High

Cvss Base Score : 10.0

Cvss Vector : AV:N/AC:L/Au:N/C:C/I:C/A:C

Description

GNU Bash through 4.3 processes trailing strings after function definitions in the values of environment variables, which allows remote attackers to execute arbitrary code via a crafted environment, as demonstrated by vectors involving the ForceCommand feature in OpenSSH sshd, the mod_cgi and mod_cgid modules in the Apache HTTP Server, scripts executed by unspecified DHCP clients, and other situations in which setting the environment occurs across a privilege boundary from Bash execution, aka "ShellShock." NOTE: the original fix for this issue was incorrect; CVE-2014-7169 has been assigned to cover the vulnerability that is still present after the incorrect fix.

Related Products

Device

Ip	Device Base Risk	Vuln Base Risk	Detection Status	Detection Type
192.168.46.12	100	100	Detected	Active
192.168.41.11	100	100	Detected	Active
192.168.47.10	100	100	Uploaded	Active
192.168.46.12	100	100	Detected	Active

Subnet

Network	Subnet Base Risk	Vuln Base Risk	Total Vuln
192.168.47.0/24	51	100	1101
192.168.41.0/24	35	100	4906
0.0.0.0/0	33	100	858

Network	Subnet Base Risk	Vuln Base Risk	Total Vuln
192.168.46.0/24	75	100	2621

Location

Business Unit

CVE-2017-0148 - Microsoft Windows SMB Server CVE-2017-0148 Remote Code Execution Vulnerability






90 (High Risk)	Exist	14	6	0	0
Base Risk	Exploitability	Device Count	Subnet Count	Location Count	Business Unit

Publish Date : 2017-03-16 21:59:04

Last Modified Date : 2019-08-27 16:22:43

Impact Values

Importance Level : High

Cvss Base Score : 9.3

Cvss Vector : AV:N/AC:M/Au:N/C:C/I:C/A:C

Description

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.

Related Products

Device

Ip	Device Base Risk	Vuln Base Risk	Detection Status	Detection Type
192.168.49.20	90	90	Uploaded	-
192.168.41.132	100	90	Detected	Both
192.168.47.2	90	90	Detected	Active
192.168.50.22	100	90	Uploaded	-
192.168.47.11	100	90	Uploaded	Active
192.168.41.10	100	90	Detected	Active
10.10.13.2	90	90	Detected	Active
192.168.50.20	100	90	Uploaded	-
192.168.43.55	100	90	Detected	Active
192.168.50.40	100	90	Uploaded	-
192.168.43.144	100	90	Detected	Passive
10.10.13.55	100	90	Detected	Active
192.168.41.131	100	90	Detected	Passive
192.168.49.22	100	90	Uploaded	-

Subnet

Network	Subnet Base Risk	Vuln Base Risk	Total Vuln
10.10.13.0/24	8	90	1798
192.168.43.0/24	33	90	2214
192.168.50.0/24	58	90	2458
192.168.49.0/24	60	90	1336
192.168.47.0/24	51	90	1101
192.168.41.0/24	35	90	4906

Location

Business Unit

CVE-2017-0146 - Microsoft Windows SMB Server CVE-2017-0146 Remote Code Execution Vulnerability






90 (High Risk)	Exist	14	6	0	0
Base Risk	Exploitability	Device Count	Subnet Count	Location Count	Business Unit

Publish Date : 2017-03-16 21:59:04

Last Modified Date : 2019-08-27 16:22:43

Impact Values

Importance Level : High

Cvss Base Score : 9.3

Cvss Vector : AV:N/AC:M/Au:N/C:C/I:C/A:C

Description

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.

Related Products

Device

Ip	Device Base Risk	Vuln Base Risk	Detection Status	Detection Type
192.168.41.131	100	90	Detected	Passive
192.168.41.10	100	90	Detected	Active
192.168.47.2	90	90	Detected	Active
192.168.49.20	90	90	Uploaded	-
192.168.43.55	100	90	Detected	Active
192.168.50.22	100	90	Uploaded	-
192.168.49.22	100	90	Uploaded	-
192.168.47.11	100	90	Uploaded	Active
192.168.50.20	100	90	Uploaded	-
10.10.13.55	100	90	Detected	Active
10.10.13.2	90	90	Detected	Active

Ip	Device Base Risk	Vuln Base Risk	Detection Status	Detection Type
192.168.41.132	100	90	Detected	Both
192.168.43.144	100	90	Detected	Passive
192.168.50.40	100	90	Uploaded	-

Subnet

Network	Subnet Base Risk	Vuln Base Risk	Total Vuln
192.168.47.0/24	51	90	1101
192.168.43.0/24	33	90	2214
10.10.13.0/24	8	90	1798
192.168.50.0/24	58	90	2458
192.168.41.0/24	35	90	4906
192.168.49.0/24	60	90	1336

Location

Business Unit

CVE-2017-0145 - Microsoft Windows SMB Server CVE-2017-0145 Remote Code Execution Vulnerability

90 (High Risk)	Exist	14	6	0	0
Base Risk	Exploitability	Device Count	Subnet Count	Location Count	Business Unit

Publish Date : 2017-03-16 21:59:04

Last Modified Date : 2019-08-27 16:22:43

Impact Values

Importance Level : High

Cvss Base Score : 9.3

Cvss Vector : AV:N/AC:M/Au:N/C:C/I:C/A:C

Description

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.

Related Products

Device

Ip	Device Base Risk	Vuln Base Risk	Detection Status	Detection Type
192.168.49.22	100	90	Uploaded	-
192.168.43.55	100	90	Detected	Active
192.168.43.144	100	90	Detected	Passive
192.168.50.40	100	90	Uploaded	-
10.10.13.55	100	90	Detected	Active
192.168.50.20	100	90	Uploaded	-
192.168.41.132	100	90	Detected	Both
192.168.50.22	100	90	Uploaded	-
192.168.49.20	90	90	Uploaded	-
192.168.41.131	100	90	Detected	Passive
10.10.13.2	90	90	Detected	Active
192.168.47.2	90	90	Detected	Active
192.168.47.11	100	90	Uploaded	Active
192.168.41.10	100	90	Detected	Active

Subnet

Network	Subnet Base Risk	Vuln Base Risk	Total Vuln
192.168.47.0/24	51	90	1101
192.168.50.0/24	58	90	2458
192.168.41.0/24	35	90	4906
192.168.43.0/24	33	90	2214
192.168.49.0/24	60	90	1336
10.10.13.0/24	8	90	1798

Location

Business Unit

CVE-2017-0144 - Microsoft Windows SMB Server CVE-2017-0144 Remote Code Execution Vulnerability






90 (High Risk)	Exist	14	6	0	0
Base Risk	Exploitability	Device Count	Subnet Count	Location Count	Business Unit

Publish Date : 2017-03-16 21:59:04

Last Modified Date : 2019-08-27 16:22:43

Impact Values

Importance Level : High

Cvss Base Score : 9.3

Cvss Vector : AV:N/AC:M/Au:N/C:C/I:C/A:C

Description

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.

Related Products

Device

Ip	Device Base Risk	Vuln Base Risk	Detection Status	Detection Type
192.168.47.2	90	90	Detected	Active
192.168.49.22	100	90	Uploaded	-
192.168.49.20	90	90	Uploaded	-
192.168.50.22	100	90	Uploaded	-
10.10.13.55	100	90	Detected	Active
192.168.41.132	100	90	Detected	Both
192.168.41.131	100	90	Detected	Passive
192.168.41.10	100	90	Detected	Active
10.10.13.2	90	90	Detected	Active
192.168.50.40	100	90	Uploaded	-
192.168.43.144	100	90	Detected	Passive

Ip	Device Base Risk	Vuln Base Risk	Detection Status	Detection Type
192.168.47.11	100	90	Uploaded	Active
192.168.43.55	100	90	Detected	Active
192.168.50.20	100	90	Uploaded	-

Subnet

Network	Subnet Base Risk	Vuln Base Risk	Total Vuln
192.168.50.0/24	58	90	2458
192.168.41.0/24	35	90	4906
192.168.43.0/24	33	90	2214
192.168.47.0/24	51	90	1101
10.10.13.0/24	8	90	1798
192.168.49.0/24	60	90	1336

Location

Business Unit

CVE-2017-0143 - Microsoft Windows SMB Server CVE-2017-0143 Remote Code Execution Vulnerability

90 (High Risk)	Exist	14	6	0	0
Base Risk	Exploitability	Device Count	Subnet Count	Location Count	Business Unit

Publish Date : 2017-03-16 21:59:03

Last Modified Date : 2019-08-27 16:22:43

Impact Values

Importance Level : High

Cvss Base Score : 9.3

Cvss Vector : AV:N/AC:M/Au:N/C:C/I:C/A:C

Description

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.

Related Products

Device

Ip	Device Base Risk	Vuln Base Risk	Detection Status	Detection Type
192.168.41.131	100	90	Detected	Passive
192.168.43.55	100	90	Detected	Active
192.168.49.20	90	90	Uploaded	-
192.168.47.2	90	90	Detected	Active
192.168.50.20	100	90	Uploaded	-
192.168.41.10	100	90	Detected	Active
192.168.49.22	100	90	Uploaded	-
192.168.47.11	100	90	Uploaded	Active
10.10.13.55	100	90	Detected	Active
192.168.41.132	100	90	Detected	Both
192.168.43.144	100	90	Detected	Passive
10.10.13.2	90	90	Detected	Active
192.168.50.40	100	90	Uploaded	-
192.168.50.22	100	90	Uploaded	-

Subnet

Network	Subnet Base Risk	Vuln Base Risk	Total Vuln
192.168.43.0/24	33	90	2214
10.10.13.0/24	8	90	1798
192.168.50.0/24	58	90	2458
192.168.47.0/24	51	90	1101
192.168.49.0/24	60	90	1336
192.168.41.0/24	35	90	4906

Location

Business Unit

Appendix

Applied Filters

Ports :	*No Filter*
Softwares :	*No Filter*
Vulnerabilities :	*CVE-2017-0148, CVE-2017-0146, CVE-2017-0145, CVE-2017-0144, CVE-2017-0143, CVE-2014-6271*
Devices :	*No Filter*
Subnets :	*No Filter*
Locations :	*No Filter*
Business Units :	*No Filter*
Vulnerability Severities :	*No Filter*
Device Severities :	*No Filter*