Symantec Incidents Report

Generated: 2026-03-04 17:34:11
Total Incidents: 559

ID	Title	Severity	Status	Created
72848402-36c0-4055-ad62-7fce345a4cb3	Exploitation for Defense Evasion [AMSI Bypass]; BITS Jobs; Command and Scripting Interpreter	Critical	New	2026-03-04
386a6968-2595-49f6-8df8-da2c319beed0	Exploitation for Defense Evasion [AMSI Bypass]; BITS Jobs; Command and Scripting Interpreter	Critical	New	2026-03-03
6ee4fb9d-a0ad-44d5-8e2f-0a91ad973647	Exploitation for Defense Evasion [AMSI Bypass]; BITS Jobs; Command and Scripting Interpreter	Critical	New	2026-03-01
22eaf124-5018-49ec-821b-1d7070b6142e	Exploitation for Defense Evasion [AMSI Bypass]; BITS Jobs; Command and Scripting Interpreter	Critical	New	2026-03-01
9ea71a78-4ad8-4ad5-a371-71c6140e3f6f	Exploitation for Defense Evasion [AMSI Bypass]; BITS Jobs; Command and Scripting Interpreter	Critical	New	2026-02-28
68abd737-1016-4fdf-97b2-13ef01828344	Exploitation for Defense Evasion [AMSI Bypass]; BITS Jobs; Command and Scripting Interpreter	Critical	New	2026-02-27
29f55ad4-a1cb-4bcd-bb62-09b4e0fc0e71	Exploitation for Defense Evasion [AMSI Bypass]; BITS Jobs; Command and Scripting Interpreter	Critical	New	2026-02-26
f16f78c3-64c2-4e3e-af63-b8e01c7d963a	inbridge-w11-G:OS Credential Dumping: Security Account Manager, Process Injection, Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder, Exfiltration Over Alternative Protocol	High	New	2026-02-25
68c141ae-fbef-48b0-823b-94edf24a86b1	Exploitation for Defense Evasion [AMSI Bypass]; BITS Jobs; Command and Scripting Interpreter	Critical	New	2026-02-25
e3355206-bbd5-4306-92d5-35fd12bfdb70	Exploitation for Defense Evasion [AMSI Bypass]; BITS Jobs; Command and Scripting Interpreter	Critical	New	2026-02-23
69df2df7-bcf6-47e7-b9db-6412e8f97525	Exploitation for Defense Evasion [AMSI Bypass]; BITS Jobs; Command and Scripting Interpreter	Critical	New	2026-02-22
7f28ef4d-d702-4d9f-85ab-940c5cf374bc	Exploitation for Defense Evasion [AMSI Bypass]; BITS Jobs; Command and Scripting Interpreter	Critical	New	2026-02-21
5e3e4495-fd41-46b4-9574-2ef9d8194508	Command and Scripting Interpreter; Disable or Modify Tools; PowerShell; Regsvr32	Critical	New	2026-02-20
10e2013b-99f7-4c97-8673-a19d0b124857	DESKTOP-P5F0K66:OS Credential Dumping: Security Account Manager, Exfiltration Over Alternative Protocol, Ingress Tool Transfer, Signed Binary Proxy Execution: Mshta	High	New	2026-02-20
306639a8-0fdf-4acf-9903-3f70b09af068	Exploitation for Defense Evasion [AMSI Bypass]; BITS Jobs; Command and Scripting Interpreter	Critical	New	2026-02-20
052dd1b0-7e88-42ff-88f8-111e2d604391	Security Account Manager	High	New	2026-02-19
e4992f50-f7fc-4ddc-891f-07f5fef4630a	Exploitation for Defense Evasion [AMSI Bypass]; BITS Jobs; Command and Scripting Interpreter	Critical	New	2026-02-18
ea262a44-969f-4264-8d39-f34acda15599	Exploitation for Defense Evasion [AMSI Bypass]; BITS Jobs; Command and Scripting Interpreter	Critical	New	2026-02-17
6e995b4b-59cc-49a0-ac0a-b7dc5cb6485f	Exploitation for Defense Evasion [AMSI Bypass]; BITS Jobs; Command and Scripting Interpreter	Critical	New	2026-02-16
b408be51-6681-407d-9c88-b820ec561957	Exploitation for Defense Evasion [AMSI Bypass]; BITS Jobs; Command and Scripting Interpreter	Critical	New	2026-02-15
79bf5312-3791-4cae-b9c6-004bc0917066	Exploitation for Defense Evasion [AMSI Bypass]; BITS Jobs; Command and Scripting Interpreter	Critical	New	2026-02-13
2d6ee9e9-734f-44c2-	Exploitation for Defense Evasion [AMSI Bypass];	Critical	New	2026-02-12

Symantec Incidents Report

ID	Title	Severity	Status	Created
b5b5-645d6cabee92	BITS Jobs; Command and Scripting Interpreter			
7eb5e991-878e-42ea-a20e-301c4144349c	Exploitation for Defense Evasion [AMSI Bypass]; BITS Jobs; Command and Scripting Interpreter	Critical	New	2026-02-12
b4c41b46-8df0-4bbc-b62a-7248b8026034	Exploitation for Defense Evasion [AMSI Bypass]; BITS Jobs; Command and Scripting Interpreter	Critical	New	2026-02-11
f86c6e18-000f-44d1-b761-9035c6be93de	Security Account Manager	High	New	2026-02-10
065bfee4-461f-4604-826d-036af2571812	Exploitation for Defense Evasion [AMSI Bypass]; BITS Jobs; Command and Scripting Interpreter	Critical	New	2026-02-10
9ae057c5-6577-4008-a338-065a71a73f71	Exploitation for Defense Evasion [AMSI Bypass]; BITS Jobs; Command and Scripting Interpreter	Critical	New	2026-02-08
589e3f40-691d-46ab-b3d0-dbfc8afd1519	Ingress Tool Transfer	Critical	New	2026-02-08
93483c13-c654-406a-bb7e-af60eede48e3	Exploitation for Defense Evasion [AMSI Bypass]; BITS Jobs; Command and Scripting Interpreter	Critical	New	2026-02-07
74b18322-f944-4f3e-8f2d-353d9878035e	DESKTOP-P5F0K66:OS Credential Dumping: Security Account Manager, Exfiltration Over Alternative Protocol, Ingress Tool Transfer, Signed Binary Proxy Execution: Msiexec	High	New	2026-02-06
76abff83-9a73-488a-ad19-a2bcd2dab111	Exploitation for Defense Evasion [AMSI Bypass]; BITS Jobs; Command and Scripting Interpreter	Critical	New	2026-02-06
f874ea29-0398-4574-bf9b-4c9732f21c3b	Exploitation for Defense Evasion [AMSI Bypass]; BITS Jobs; Command and Scripting Interpreter	Critical	New	2026-02-05
50cbf1cb-4d8a-4398-9dcb-8b92a3d4413f	Exploitation for Defense Evasion [AMSI Bypass]; Account Manipulation; BITS Jobs	Critical	New	2026-02-04
35e525b7-1046-4ff1-a409-2bdcf6ab7057	Exploitation for Defense Evasion [AMSI Bypass]; Accessibility Features; Account Manipulation	Critical	New	2026-02-03
66b88739-faec-42a0-9cf0-3b1c154b4858	inbridge-w11-G:Signed Binary Proxy Execution: Mshta, Impair Defenses: Disable or Modify Tools, Command and Scripting Interpreter: PowerShell, Command and Scripting Interpreter	High	New	2026-02-03
8c861f1a-b492-425f-9f01-1f2511a037ee	Exploitation for Defense Evasion [AMSI Bypass]; Accessibility Features; Account Manipulation	Critical	New	2026-02-03
c748d817-0e3a-4349-aa3a-166773967a4d	Exploitation for Defense Evasion [AMSI Bypass]; Accessibility Features; Account Manipulation	Critical	New	2026-02-03
5398933a-45e2-4846-8659-9cdfefcd0d52	Exploitation for Defense Evasion [AMSI Bypass]; Accessibility Features; Account Manipulation	Critical	New	2026-02-03
305addc9-eeae-43ab-8016-02920ef23f9f	inbridge-w11-05:OS Credential Dumping: NTDS, OS Credential Dumping: Security Account Manager, Process Injection, Exfiltration Over Alternative Protocol	High	New	2026-02-02
0b146410-23ed-44eb-8031-a4b86026de0c	inbridge-w11-G:Signed Binary Proxy Execution: Mshta, Impair Defenses: Disable or Modify Tools, Command and Scripting Interpreter: PowerShell, Command and Scripting Interpreter	High	New	2026-02-02
18bcc3d6-725b-4e6f-94ea-2d6d11746c02	inbridge-w11-05:OS Credential Dumping: Security Account Manager, Process Injection, Exfiltration Over Alternative Protocol, Ingress Tool Transfer	High	New	2026-02-02
c487a326-8b5c-48df-b76f-1d1f36fdc1dd	Exploitation for Defense Evasion [AMSI Bypass]; Accessibility Features; Account Manipulation	Critical	New	2026-02-02
309a87d2-301f-46d1-be68-52cba546bf11	Exploitation for Defense Evasion [AMSI Bypass]; Accessibility Features; Account Manipulation	Critical	New	2026-02-02
ec0231f0-	Ingress Tool Transfer; Security Software	Critical	New	2026-02-02

Symantec Incidents Report

ID	Title	Severity	Status	Created
ff45-4e09-92ac-831092c0b6a7	Discovery			
a1247cac-25a4-4515-9141-01080b3f1ca2	inbridge-w11-05:OS Credential Dumping, OS Credential Dumping: Security Account Manager, Exfiltration Over Alternative Protocol, Ingress Tool Transfer	High	New	2026-02-02
9eae843a-8a2e-4b07-b79b-0c9ee57479d8	Exploitation for Defense Evasion [AMSI Bypass]; Account Manipulation; BITS Jobs	Critical	New	2026-02-02
37caf334-086a-417a-b577-2cf007e1993c	inbridge-w11-05:OS Credential Dumping: NTDS, OS Credential Dumping: Security Account Manager, Exfiltration Over Alternative Protocol, Ingress Tool Transfer	High	New	2026-02-02
47d0b2f5-696b-42af-8389-a4b8d130b9ae	Exploitation for Defense Evasion [AMSI Bypass]; Account Manipulation; BITS Jobs	Critical	New	2026-02-01
153daf2f-12be-4ab1-a224-6cc5821c66d5	Exploitation for Defense Evasion [AMSI Bypass]; Account Manipulation; BITS Jobs	Critical	New	2026-02-01
5b99b4a5-ec02-4055-bbd4-642586cb9146	inbridge-w11-05:OS Credential Dumping: NTDS, OS Credential Dumping: Security Account Manager, Process Injection, Exfiltration Over Alternative Protocol	High	New	2026-02-01
5ecce58b-eea0-4ca0-8d10-2fddfd2cea46	inbridge-w11-G:Signed Binary Proxy Execution: Mshta, Trusted Developer Utilities Proxy Execution: MSBuild, BITS Jobs, Command and Scripting Interpreter: PowerShell	High	New	2026-02-01
8720f5c0-ca75-4fab-bd4c-bddeafff54c4	Exploitation for Defense Evasion [AMSI Bypass]; Account Manipulation; BITS Jobs	Critical	New	2026-02-01
f1b5fb40-ca3b-482b-8553-3668460a5fb4	inbridge-w11-05:OS Credential Dumping: NTDS, OS Credential Dumping: Security Account Manager, Process Injection, Exfiltration Over Alternative Protocol	High	New	2026-02-01
8bdcd850-01a7-48b8-b2ec-f6fad988d71b	Exploitation for Defense Evasion [AMSI Bypass]; Account Manipulation; BITS Jobs	Critical	New	2026-02-01
4830b9cc-9999-4a5c-b57b-2a80690971c2	Exploitation for Defense Evasion [AMSI Bypass]; Account Manipulation; BITS Jobs	Critical	New	2026-02-01
d4212718-7a31-493e-a1be-75ceef3cbd89	Exploitation for Defense Evasion [AMSI Bypass]; Account Manipulation; BITS Jobs	Critical	New	2026-02-01
5b1fbf83-30d5-480b-985d-76ce5402dd5c	Account Manipulation; BITS Jobs; Command and Scripting Interpreter; Disable or Modify Tools	Critical	New	2026-02-01
774f38b4-ea3c-4554-8eb2-3ef07889496d	inbridge-w11-05:OS Credential Dumping: NTDS, OS Credential Dumping: Security Account Manager, Exfiltration Over Alternative Protocol, Ingress Tool Transfer	High	New	2026-02-01
710acb4a-defc-42d1-9df7-adddf83c57f5	Exploitation for Defense Evasion [AMSI Bypass]; OS Credential Dumping [Mimikatz]	Critical	New	2026-01-31
01e12163-195b-4e23-86fd-bb4a41a6d5b7	inbridge-w11-05:OS Credential Dumping: NTDS, OS Credential Dumping: Security Account Manager, Process Injection, Exfiltration Over Alternative Protocol	High	New	2026-01-31
1a7b897a-440d-4474-b8c2-f7588c6af148	Exploitation for Defense Evasion [AMSI Bypass]; OS Credential Dumping [Mimikatz]	Critical	New	2026-01-31
e923db0b-8633-41cf-a259-dd188ff7c445	Exploitation for Defense Evasion [AMSI Bypass]; OS Credential Dumping [Mimikatz]	Critical	New	2026-01-31
63301866-c656-45b4-85a0-269a75ef7dd9	Exploitation for Defense Evasion [AMSI Bypass]; OS Credential Dumping [Mimikatz]	Critical	New	2026-01-31
2cf928cc-c9b7-4ba5-8054-fc670cf87725	inbridge-w11-05:OS Credential Dumping: NTDS, OS Credential Dumping: Security Account Manager, Process Injection, Exfiltration Over	High	New	2026-01-31

Symantec Incidents Report

ID	Title	Severity	Status	Created
	Alternative Protocol			
0f64f19f-1112-49d3-9f51-813cf5dd08ef	Exploitation for Defense Evasion [AMSI Bypass]; OS Credential Dumping [Mimikatz]	Critical	New	2026-01-31
02ca58d0-1f4f-4037-9a0e-70e79df8f344	inbridge-w11-05:OS Credential Dumping: Security Account Manager, Exfiltration Over Alternative Protocol, Ingress Tool Transfer, Signed Binary Proxy Execution: Msiexec	High	New	2026-01-31
027fc8d4-f892-48f6-8382-82b2be36eecc	Exploitation for Defense Evasion [AMSI Bypass]; OS Credential Dumping [Mimikatz]	Critical	New	2026-01-31
e0a4c56a-3a89-42a0-b6ab-da38bacb25c8	Exploitation for Defense Evasion [AMSI Bypass]; OS Credential Dumping [Mimikatz]	High	New	2026-01-30
5ccd4e85-d134-415f-8b9f-756f33a707d0	Exploitation for Defense Evasion [AMSI Bypass]; Account Manipulation; BITS Jobs	Critical	New	2026-01-30
17cf5aaa-85dc-482b-8083-be302597d2c2	inbridge-w11-05:OS Credential Dumping: Security Account Manager, Exfiltration Over Alternative Protocol, Ingress Tool Transfer, Signed Binary Proxy Execution: Msiexec	High	New	2026-01-30
034c8d35-e8d3-4f67-bf77-5ddd8f70596f	Exploitation for Defense Evasion [AMSI Bypass]; Account Manipulation; BITS Jobs	Critical	New	2026-01-30
6e880d77-82ac-433c-95bd-16b9ef25e04d	inbridge-w11-05:OS Credential Dumping: NTDS, OS Credential Dumping: Security Account Manager, Scheduled Task/Job: At (Windows), Exfiltration Over Alternative Protocol	High	New	2026-01-30
f846846b-f55c-4bc0-a126-3b60ecdaa981	Exploitation for Defense Evasion [AMSI Bypass]; Account Manipulation; BITS Jobs	Critical	New	2026-01-30
28d4b3c6-de74-4e02-8dc8-ae0d76511b17	Exploitation for Defense Evasion [AMSI Bypass]; Account Manipulation; BITS Jobs	Critical	New	2026-01-30
ffbd5a8e-0578-4820-a22f-ba21750677a4	inbridge-w11-05:OS Credential Dumping: NTDS, OS Credential Dumping: Security Account Manager, Process Injection, Exfiltration Over Alternative Protocol	High	New	2026-01-30
2e6ab01a-991f-4e85-af54-8a46ed65b1e8	inbridge-w11-G:Signed Binary Proxy Execution: Mshta, Trusted Developer Utilities Proxy Execution: MSBuild, Signed Binary Proxy Execution: Rundll32, Impair Defenses: Disable or Modify Tools	High	New	2026-01-29
c1c79fca-4831-43e7-a531-04c0ae02919f	inbridge-w11-05:OS Credential Dumping: NTDS, OS Credential Dumping: Security Account Manager, Process Injection, Exfiltration Over Alternative Protocol	High	New	2026-01-29
9dcbae7b-f4dd-4c2e-89b8-13adc9365f84	Exploitation for Defense Evasion [AMSI Bypass]; Account Manipulation; BITS Jobs	Critical	New	2026-01-29
890c3e03-b69a-42a7-8627-62b5bdf2a080	Exploitation for Defense Evasion [AMSI Bypass]; Account Manipulation; BITS Jobs	Critical	New	2026-01-29
c16188cd-97c2-496f-a81f-c048363eb63c	Exploitation for Defense Evasion [AMSI Bypass]; Account Manipulation; BITS Jobs	Critical	New	2026-01-29
88920992-184b-4f85-a614-710de5963099	inbridge-w11-05:OS Credential Dumping: NTDS, OS Credential Dumping: Security Account Manager, Process Injection, Exfiltration Over Alternative Protocol	High	New	2026-01-29
2bd24e90-c541-40f2-8af3-e0eba30d368c	Exploitation for Defense Evasion [AMSI Bypass]; Account Manipulation; BITS Jobs	Critical	New	2026-01-29
2450dcd6-9c40-4a6b-98df-8e	Exploitation for Defense Evasion [AMSI Bypass];	Critical	New	2026-01-29

Symantec Incidents Report

ID	Title	Severity	Status	Created
de30c063a4	Account Manipulation; BITS Jobs			
24019e8c-bbb1-4d8d-9ac7-fb7dd4192681	Exploitation for Defense Evasion [AMSI Bypass]; Account Manipulation; BITS Jobs	Critical	New	2026-01-29
dfd3d2f2-544e-4462-8f7d-f1c05b6995b9	inbridge-w11-05:OS Credential Dumping: NTDS, OS Credential Dumping: Security Account Manager, Process Injection, Exfiltration Over Alternative Protocol	High	New	2026-01-29
99aa480e-aeb4-4bd9-b077-63917688b8d5	Exploitation for Defense Evasion [AMSI Bypass]; Account Manipulation; BITS Jobs	Critical	New	2026-01-28
58aa4352-e62a-4667-aed6-d6c7a25c79d9	inbridge-w11-05:OS Credential Dumping: Security Account Manager, Process Injection, Exfiltration Over Alternative Protocol, Ingress Tool Transfer	High	New	2026-01-28
54dab194-0c8b-4fca-a9e9-1f905b91fce0	Exploitation for Defense Evasion [AMSI Bypass]; Account Manipulation; BITS Jobs	Critical	New	2026-01-28
3f47443e-a94b-462a-9098-2386888f8458	Exploitation for Defense Evasion [AMSI Bypass]; Account Manipulation; BITS Jobs	Critical	New	2026-01-28
c5fe78a8-d5de-42ad-8292-d4fbfe375f98	Exploitation for Defense Evasion [AMSI Bypass]; Account Manipulation; BITS Jobs	Critical	New	2026-01-28
101dc60b-0d4b-4826-be3a-1ad41eab6208	Exploitation for Defense Evasion [AMSI Bypass]; Account Manipulation; BITS Jobs	Critical	New	2026-01-28
78bc52d2-17b8-41b8-9ffc-e882e348f168	inbridge-w11-05:OS Credential Dumping: NTDS, OS Credential Dumping: Security Account Manager, Process Injection, Exfiltration Over Alternative Protocol	High	New	2026-01-28
495699b7-8fa0-4418-b1b6-01f7f4b1df55	Exploitation for Defense Evasion [AMSI Bypass]; Account Manipulation; BITS Jobs	Critical	New	2026-01-28
3a9479f5-fc6c-49ee-aaa1-543c2675a3c8	Exploitation for Defense Evasion [AMSI Bypass]; Account Manipulation; BITS Jobs	Critical	New	2026-01-28
601aa692-876d-4ca8-bf13-a52bfa4c979a	Exploitation for Defense Evasion [AMSI Bypass]; Account Manipulation; BITS Jobs	Critical	New	2026-01-28
2e142152-fd76-4ac8-8026-a9cfa65c65dd	inbridge-w11-05:OS Credential Dumping: NTDS, OS Credential Dumping: Security Account Manager, Exfiltration Over Alternative Protocol, Ingress Tool Transfer	High	New	2026-01-28
a30d4e85-017f-4689-abc2-4c01baae5be6	Exploitation for Defense Evasion [AMSI Bypass]; Account Manipulation; BITS Jobs	Critical	New	2026-01-27
bba85adc-5bdf-4871-8943-828285f1f2b2	inbridge-w11-05:OS Credential Dumping: NTDS, OS Credential Dumping: Security Account Manager, Process Injection, Exfiltration Over Alternative Protocol	High	New	2026-01-27
950769f9-79fe-4fc8-aff4-1ab45b286754	Exploitation for Defense Evasion [AMSI Bypass]; Account Manipulation; BITS Jobs	Critical	New	2026-01-27
5655850d-4bf5-493c-9925-9decd92891b6	Exploitation for Defense Evasion [AMSI Bypass]; Account Manipulation; BITS Jobs	Critical	New	2026-01-27