

The background of the page is a complex network visualization with glowing blue nodes and connecting lines, set against a dark background. Some nodes are labeled with numbers like 2789, 3659, 4617, and 5013.

Newscast Critical vulnerability in Symantec

Table of content

SYMANTEC	2
CVE-2024-23613	2
Type of vulnerability	2
Risks.....	2
Severity (base score CVSS 3.1)	2
Impacted Products.....	2
Recommendations.....	2
Proof of concept.....	2
CVE-2024-23614	3
Type of vulnerability	3
Risks.....	3
Severity (base score CVSS 3.1)	3
Impacted Products.....	3
Recommendations.....	3
Proof of concept.....	3
CVE-2024-23615	4
Type of vulnerability	4
Risks.....	4
Severity (base score CVSS 3.1)	4
Impacted Products	4
Recommendations.....	4
Proof of concept.....	4
CVE-2024-23616	5
Type of vulnerability	5
Risks.....	5
Severity (base score CVSS 3.1)	5
Impacted Products	5
Recommendations.....	5
Proof of concept.....	5
SOURCES	6

Symantec

On 25 January 2024, Exodus Intelligence published four security advisories concerning the critical vulnerabilities [CVE-2024-23613](#), [CVE-2024-23614](#), [CVE-2024-23615](#) and [CVE-2024-23616](#) in Symantec.

CVE-2024-23613



This vulnerability is due to a memory control flaw when parsing Symantec Deployment Solution's *UpdateComputer* tokens.

By sending specially crafted requests, an unauthenticated attacker can execute arbitrary code with *SYSTEM* privileges.

Type of vulnerability

- [CWE-119](#): Improper Restriction of Operations within the Bounds of a Memory Buffer

Risks

- Remote code execution
- Privilege escalation

Severity (base score CVSS 3.1)

Attack vector	Network	Scope	Unchanged
Attack complexity	Low	Impact on confidentiality	High
Privileges Required	None	Impact on integrity	High
User Interaction	None	Impact on availability	High

Impacted Products

- According to Exodus Intelligence, only Symantec Deployment Solution version 7.9 is impacted.

Recommendations

- As this product has reached end-of-life, no patch is available.
- It is recommended to use a product that is still receiving security updates.
- Additional information is available in Exodus Intelligence's [security advisory](#).

Proof of concept

To date, no proof of concept is available in open source.

CVE-2024-23614



This vulnerability is due to a memory control flaw in Symantec Messaging Gateway.

By sending specially crafted requests, an unauthenticated attacker can execute arbitrary code as *root*.

Type of vulnerability

- **CWE-119**: Improper Restriction of Operations within the Bounds of a Memory Buffer

Risks

- Remote code execution
- Privilege escalation

Severity (base score CVSS 3.1)

Attack vector	Network	Scope	Unchanged
Attack complexity	Low	Impact on confidentiality	High
Privileges Required	None	Impact on integrity	High
User Interaction	None	Impact on availability	High

Impacted Products

- According to Exodus Intelligence, only Symantec Messaging Gateway versions 9.5 and earlier are impacted.

Recommendations

- As this product has reached end-of-life, no patch is available.
- It is recommended to use a product that is still receiving security updates.
- Additional information is available in Exodus Intelligence's [security advisory](#).

Proof of concept

To date, no proof of concept is available in open source.

CVE-2024-23615



This vulnerability is due to a memory control flaw in Symantec Messaging Gateway.

By sending specially crafted requests, an unauthenticated attacker can execute arbitrary code as *root*.

Type of vulnerability

- **CWE-119**: Improper Restriction of Operations within the Bounds of a Memory Buffer

Risks

- Remote code execution
- Privilege escalation

Severity (base score CVSS 3.1)

Attack vector	Network	Scope	Unchanged
Attack complexity	Low	Impact on confidentiality	High
Privileges Required	None	Impact on integrity	High
User Interaction	None	Impact on availability	High

Impacted Products

- According to Exodus Intelligence, only Symantec Messaging Gateway versions 9.5 and earlier are impacted.

Recommendations

- As this product has reached end-of-life, no patch is available.
- It is recommended to use a product that is still receiving security updates.
- Additional information is available in Exodus Intelligence's [security advisory](#).

Proof of concept

To date, no proof of concept is available in open source.

CVE-2024-23616



This vulnerability is due to a memory control flaw in Symantec Server Management Suite.

By sending specially crafted requests, an unauthenticated attacker can execute arbitrary code with *SYSTEM* privileges.

Type of vulnerability

- **CWE-119**: Improper Restriction of Operations within the Bounds of a Memory Buffer

Risks

- Remote code execution
- Privilege escalation

Severity (base score CVSS 3.1)

Attack vector	Network	Scope	Unchanged
Attack complexity	Low	Impact on confidentiality	High
Privileges Required	None	Impact on integrity	High
User Interaction	None	Impact on availability	High

Impacted Products

- According to Exodus Intelligence, only Symantec Server Management Suite version 7.9 and earlier are impacted.

Recommendations

- As this product has reached end-of-life, no patch is available.
- It is recommended to use a product that is still receiving security updates.
- Additional information is available in Exodus Intelligence's [security advisory](#).

Proof of concept

To date, no proof of concept is available in open source.

Sources

CVE-2024-23613

- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-23613>
- <https://blog.exodusintel.com/2024/01/25/symantec-deployment-solution-axengine-exe-buffer-overflow-remote-code-execution/>

CVE-2024-23614

- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-23614>
- <https://blog.exodusintel.com/2024/01/25/symantec-messaging-gateway-stack-buffer-overflow-remote-code-execution/>

CVE-2024-23615

- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-23615>
- <https://blog.exodusintel.com/2024/01/25/symantec-messaging-gateway-libdec2lha-so-stack-buffer-overflow-remote-code-execution/>

CVE-2024-23616

- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-23616>
- <https://blog.exodusintel.com/2024/01/25/symantec-server-management-suite-axengine-exe-buffer-overflow-remote-code-execution/>