# MW6 Aztec, DataMatrix, and MaxiCode ActiveX controls versions before 4.0 are vulnerable to arbitrary code via crafted HTML document.

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

## Summary

| | |
|---|---|
| **CVE** | CVE-2013-6040 |
| **State** | PUBLISHED |
| **Assigner** | certcc |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2014-01-21 01:55:03 UTC |
| **Updated** | 2026-04-29 01:13:23 UTC |
| **Description** | MW6 Aztec, DataMatrix, and MaxiCode ActiveX controls before version 4.0 vulnerable to arbitrary code via a crafted HTML |

## Risk And Classification

**Primary CVSS:** v3.1 8.1 HIGH from ADP

CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

**EPSS:** 0.071330000 probability, percentile 0.915790000 (date 2026-05-03)

**Problem Types:** NVD-CWE-noinfo | CWE-94: Improper Control of Generation of Code

| Version | Source | Type | Score | Severity | Vector |
|---|---|---|---|---|---|
| 3.1 | ADP | DECLARED | 8.1 | HIGH | CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H |
| 3.1 | 134c704f-9b21-4f2e-91b3-4a467353bcc0 | Secondary | 8.1 | HIGH | CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H |
| 2.0 | nvd@nist.gov | Primary | 9.3 | | AV:N/AC:M/Au:N/C:C/I:C/A:C |

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

None

User Interaction

None

Scope

Unchanged

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

## CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

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

## NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Application | Mw6tech | Aztec Activex Control | - | All | All | All |
| Application | Mw6tech | Datamatrix Activex Control | - | All | All | All |
| Application | Mw6tech | Maxicode Activex Control | - | All | All | All |

## Vendor Declared Affected Products

| Source | Vendor | Product | Version | Platforms |
|---|---|---|---|---|
| CNA | MW6 Tech | MW6 Aztec ActiveX Controls | affected 0.0 4.0 custom | Not specified |
| CNA | MW6 Tech | MW6 DataMatrix ActiveX Controls | affected 0.0 4.0 custom | Not specified |
| CNA | MW6 Tech | MW6 MaxiCode ActiveX Controls | affected 0.0 4.0 custom | Not specified |

## References

| Reference | Source |
|---|---|
| Vulnerability Note VU#219470 - MW6 Technologies ActiveX controls contain multiple vulnerabilities | af854a3a-2127-422b-91ae-364da26611 |
| MW6 Technologies Aztec ActiveX (Data param) - Buffer Overflow | af854a3a-2127-422b-91ae-364da26611 |

| | |
|---|---|
| MW6 Technologies Aztec ActiveX (Data param) - Buffer Overflow | af854a3a-2127-422b-91ae-364da26611 |
| MW6 Technologies DataMatrix ActiveX (Data param) - Buffer Overflow | af854a3a-2127-422b-91ae-364da26611 |
| www.mw6tech.com | cret@cert.org |
| CVE Program record | CVE.ORG |
| NVD vulnerability detail | NVD |

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.